Universidad Carlos III de Madrid

MÁSTER UNIVERSITARIO EN BIBLIOTECAS Y SERVICIOS DE INFORMACIÓN DIGITALES

Trabajo Fin de Máster

Aspectos Jurídicos sobre la Privacidad en las Redes Sociales

Autor: **Beatriz Herce Ruiz**
Directora: **Dra. Almudena Alcaide Raya**
Fecha de presentación: **Octubre 2012**

Contenido

Tabla de Ilustraciones

Resumen

Este trabajo aborda una visión global de la situación de las redes sociales en relación a los aspectos legales relacionados con la privacidad, un concepto cuestionado tanto por los usuarios como por las organizaciones públicas y entidades privadas por la escasa protección de una serie de derechos que están protegidos desde el punto de vista jurídico; sin embargo estos medios sociales no están exentos de riesgos ni ataques malintencionados ya que publicar , compartir o transmitir una información a terceros puede poner en peligro nuestra seguridad y privacidad.

Hemos enfocado el proyecto desde una perspectiva que nos permita conocer con la normativa vigente como están regulados estos derechos en relación con las redes sociales tanto en nuestro país como en Europa; además de analizar cuáles son las medidas que adquieren estas herramientas para garantizar el acceso seguro en sus políticas de privacidad incluyendo cuáles son las mayores vulnerabilidades que poseen y que efectos producen en la privacidad de los individuos.

1. Introducción

En este capítulo abordamos la presentación del proyecto donde exponemos él porque hemos realizado este trabajo ,así como los objetivos y la metodología que hemos llevado a cabo para la realización de la memoria.

1.1 Motivación del TFM

En los últimos años estamos siendo testigos de la proliferación de los medios sociales, un fenómeno que se ha ido instaurando de forma directa en los usuarios y se ha convertido en un elemento importante para comunicarse con otras personas.
Ha supuesto una revolución en todos los sentidos, no es necesario salir de casa para establecer una conversión con un conocido e incluso desconocido, además de poder compartir datos, imágenes, estados de ánimo, fotos, archivos, buscar trabajo, expresar opiniones , etc. Lo que por un lado puede repercutir de forma beneficiosa también entraña algunos riesgos para los usuarios, a veces de manera inconsciente esto puede ser perjudicial para la intimidad e incluso para la integridad de las personas.

Al margen de los beneficios que nos están presentando las redes sociales todavía quedan algunos aspectos pendientes de revisión y de actualización como la privacidad y seguridad que nos ofrecen estos medios Web; muy pocos usuarios son los que acceden a estas herramientas teniendo un conocimiento amplio de las políticas de privacidad y de las garantías que nos ofrecen a la hora de tratar los datos que constantemente vamos insertando como contenido dinámico pero casi todos hoy en día estamos volcados en tener perfiles online y estar permanentemente conectados aún a sabiendas de las posibles repercusiones que pueden tener las informaciones que enviamos y hacemos caso omiso a las advertencias que se nos hacen desde las instituciones sobre las consecuencias de informatizar datos en las redes sociales y de la mala praxis que algunos usuarios hacen. Esto conlleva a convertir a las redes en un complejo entramado de relaciones entre diversos miembros en el que las consecuencias sobre la privacidad marcan un punto y aparte en la sociabilidad, en la confidencialidad y en la intimidad de los individuos y las redes sociales. Por ello, debido a esta debilidad aparente que presentan las redes sociales en estas cuestiones y que principalmente es provocada por todos los elementos que participan en la red social; además de la escasa legislación

vigente tanto a nivel nacional , europeo e internacional y de los recurrentes parches legales que los estados presentan sobre las políticas de acceso e uso de dichos medios y que se pone de manifiesto en las continuas noticias sobre la falta de privacidad y seguridad con las que atentan algunas redes sociales frente a los usuarios hemos intentado asociar este debate a nuestro trabajo adentrándonos en el conflicto que presentan para conocer más de cerca y profundamente los aspectos que se atañen y que se estudian sobre la privacidad y seguridad que muchas veces quedan en entredicho porque muchas veces los fines de estas alcanzan una dimensión distinta al fin para el que fueron creadas ,como la gran ingente penetración de delitos informáticos , robos de confidencialidad o fraude u otras como el robo de información valiosa sobre la vida privada , todas ellas prácticas poco éticas y incluso ilegales.

Son herramientas poderosas y muy complejas de analizar pero la dimensión que han adquirido en nuestra sociedad nos hace que profundicemos más sobre aspectos desconocidos pero que están ahí y que son difíciles de detectar y para los que incluso muchas legislaciones nacionales e internacionales todavía no lo prevén en sus normativas quedando un vacío legal que afecta también a nivel tecnológico debido a la novedad que han supuesto estas herramientas en la Sociedad de la Información. Su poder de persuadir y de mover masas nos ha motivado a adentrarnos más en el mundo de las redes sociales desde otro punto de vista, en el que conozcamos más su columna vertebral, sus mecanismos de privacidad y las tendencias más actuales en materia de protección de los usuarios.

1.2 Objetivos

El objetivo principal del presente Trabajo Fin de Máster es por un lado analizar aspectos sobre la privacidad y seguridad que se llevan a cabo en las Redes Sociales desde diversas perspectivas; contextualizando el proyecto dentro del marco legal vigente en materia jurídica al que están sometidas las Redes Sociales en las diversas jurisdicciones tanto a nivel nacional como Europeo, además de analizar otros países como Estados Unidos y algunos de América Latina través de los cuales hemos podido tener una idea más clara de las legislaciones más actuales y novísimas en materia de redes sociales.

De esta manera hemos tratado de acercarnos más si cabe a estos medios de comunicación conociendo sus entramados en cuestiones de privacidad y seguridad, aspectos que en algunas ocasiones son ajenos tanto para usuarios como para productores de servicios de redes sociales. Acercarse a sus políticas de privacidad nos hace comprender mejor la finalidad de dichos medios, nos invita a conocer más sus funcionalidades y a tomar conciencia de hasta donde un usuario puede dar a conocer datos personales que afecten a su intimidad; y a los responsables de dichos servicios a tomar el timón de la responsabilidad que conlleva que millones de usuarios de todo el mundo depositen su confianza ofreciendo datos privados en estos medios sociales ; por ello deben mostrar mejores perspectivas en cuanto al análisis de la privacidad de la información y garantizar su seguridad con herramientas tecnológicas colaborando con la legislación que se vaya formulando en cada momento.

La gran controversia en el mundo de las redes sociales y de las legislaciones vigentes es un síntoma del desconcierto que existe y de la precariedad del asunto en cuanto a esta materia. Nosotros en este trabajo pretendemos señalar aquellos aspectos jurídicos que afectan a la privacidad y que son desconocidos para la mayoría del gran público e incluso de los usuarios que con frecuencia acceden a estos medios. La mayoría de nosotros desconocemos como la ley ampara el uso o acceso a estas herramientas y como los usuarios estamos protegidos ante las agresiones virtuales a los que se ven sometidos nuestros datos personales, fotos e comentarios que nosotros vertemos en estos servicios Web y que en algunos casos atentan contra la intimidad personal .

Así pues los objetivos globales a los que va dirigido nuestro planeamiento a lo largo del documento, son los siguientes:

- Hacer un estudio identificando los aspectos jurídicos que hagan referencia a la privacidad y seguridad de las redes sociales.
- Conocer los derechos y los límites de los usuarios ante este tipo de medios de comunicación.
- Determinar cuáles son las obligaciones y responsabilidades de los prestadores de servicios de redes sociales.

- Determinar los riesgos y amenazas que se presentan en cuanto a la privacidad de la información.
- Conocer cuáles son las herramientas tecnológicas que establecen o marcan los límites para garantizar la privacidad en las redes sociales.

1.3 Metodología

La **metodología** que hemos empleado para el diseño del presente trabajo, es intentar ofrecer una panorámica actual de la situación legal a través del análisis de aspectos jurídicos que afectan a la seguridad y privacidad de estos servicios Web, tanto en el marco nacional como europeo de la forma más exhaustiva posible incluyendo un análisis global del contexto en el que se engloban las redes sociales y sus políticas de privacidad. No pretendemos ser un manual exhaustivo sobre legislación en redes sociales sino establecer un pequeño acercamiento a la naturaleza jurídica que se desarrolla en materia de seguridad y privacidad que nos permita conocer aspectos de carácter social y tecnológico lo más fidedignamente posible sobre el fenómeno de las redes sociales.

Definiremos términos, nombraremos herramientas y señalaremos iniciativas sobre legislación en materia de privacidad y de seguridad; en este sentido el trabajo no pretende ser eminentemente práctico sino más bien un estudio donde examinamos y desarrollamos la situación del marco jurídico en el que se engloban las redes sociales y del estado de la privacidad y la seguridad como agentes de suma importancia en estas herramientas de participación colaborativa.

1.4 Estructura de Capítulos

La presente memoria está estructurada en los siguientes capítulos:

En el **Capítulo 1**, se hace referencia a la introducción del proyecto donde se incluye la motivación que nos ha llevado a realizar el proyecto, los objetivos que se pretenden conseguir y cuál es la metodología que se ha empleado para su desarrollarlo.

En el **Capítulo 2**, se intenta hacer un enfoque sobre la situación de las redes sociales y la relación de estas plataformas con la privacidad. También mostramos y analizamos los derechos que son vulnerables y los datos privados que son vulnerados en los distintos ámbitos de la vida de un individuo, así como las amenazas y delitos que pueden provocarse en las redes sociales afectando a la privacidad de un individuo y de terceras personas ajenas a estos medios sociales.

En el **Capítulo 3,** se hace un recorrido más profundo sobre la legislación a la que se hace alusión en los puntos anteriores sobre los distintos aspectos jurídicos que se han analizado y que corresponden a los ámbitos que se enuncian a continuación:

- Protección de los derechos al honor, propia imagen e intimidad.
- Protección de datos de carácter personal
- Protección de la propiedad intelectual e industrial
- Protección de menores de edad.

En el **Capítulo 4**, hemos hecho mención a algunas de las tecnologías que podrían ser garantes de privacidad en el uso de acceso y comunicación en las redes sociales, algunas de las que citamos se pueden integrar otras no.

Y por último, en el **Capítulo 5** y **Capítulo 6**, realizamos las conclusiones al presente trabajo y cuestiones futuras sobre aspectos que quedan sin analizar respecto a las redes sociales y la privacidad.

2. Las Redes Sociales: Un cambio de paradigma en la privacidad

En este capítulo hacemos un recorrido por la historia de las redes sociales, así como por los derechos y datos más vulnerados en este tipo de medios sociales. También mencionamos las amenazas y delitos que conlleva el acceso y participación en estas plataformas.

2.1 Definición e Historia de las redes sociales

Las redes sociales "*son servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado*"(INTECO,2009).También, el Director de la Agencia Española de Protección de Datos define a la red social "*como una aplicación online que permite a los usuarios generar un perfil con sus datos en páginas personales y compartidos con otras personas, haciendo pública esta información, lo que potencia la interrelación con otros usuarios a partir de los perfiles publicados. Es una herramienta que facilita las relaciones sociales* ". En el Observatorio Tecnológico del Ministerio de Educación, Cultura y Deporte se define una red social como" *una estructura social formada por personas o entidades conectadas y unidas entre sí por algún tipo de relación o interés común*".

En los últimos años la eclosión de las redes sociales en Internet es la consecuencia de la progresión de la Web 2.0 y sus nuevas aplicaciones. Estas plataformas cada día experimentan una nueva crecida en el número de usuarios convirtiéndose en un punto de partida para establecer contacto y una vía de comunicación desde distintos lugares físicos entre diferentes personas; siendo hoy en día el canal de comunicación más activo entre los usuarios de todo el mundo para mantener conversaciones o compartir datos personales. Todos conocemos las ventajas derivadas de las redes sociales pero poco sobre los contras y dudas que presentan entorno a su utilización. En un mundo cambiante la tecnología sufre también sus avances, en el caso de estos medios sociales han transformado los hábitos comunicativos en diversos ámbitos sociales. Estos canales de comunicación e interacción permiten agrupar usuarios de distintos grupos e intereses

ya pueden ser por temas de ocio, a nivel profesional o simplemente como entretenimiento. Dado el crecimiento exponencial y el desarrollo de las redes sociales a lo largo de la última década, presentamos a continuación una pequeña infografía representativa sobre el origen y la evolución de estas desde sus comienzos hasta a la actualidad, donde se puede observar como con los años han ido proliferando nuevas redes sociales y desde luego muchas de ellas se han hecho un hueco para quedarse dado el grado de aceptación que tienen por parte de los usuarios.

A continuación, vamos a hacer una breve descripción de la historia de las redes sociales desde sus orígenes y como han evolucionados desde su origen en 1978 hasta el 2012 a través de la Figura 1 desde que Cristhensen y Suess inventan un sistema de comunicación para compartir información entre amigos sobre eventos o anunciar informaciones hasta ya en la última década donde observamos cómo van surgiendo las redes sociales más avanzadas como es el caso de Facebook que surge como una plataforma universitaria que crean dos estudiantes de Harvard y cuyo dueño actual Mark Zuckerberg pagó entorno a 10 millones de dólares por adquirirla .Otro hito importante en la historia de las redes sociales es la creación de Youtube en 2005 , plataforma social donde millones de usuarios comparten vídeos de diversa índole, es considerada una de las redes sociales con más participación junto con Twitter que nació en el 2006 y que tiene más de 400 millones de búsquedas al día y Facebook con 200 millones de usuarios en todo el mundo ; ambas son el referente de las redes sociales actuales por el nivel de participación y ser el modelo a seguir por todas las redes sociales en cuanto a políticas de privacidad como mecanismos de acceso.

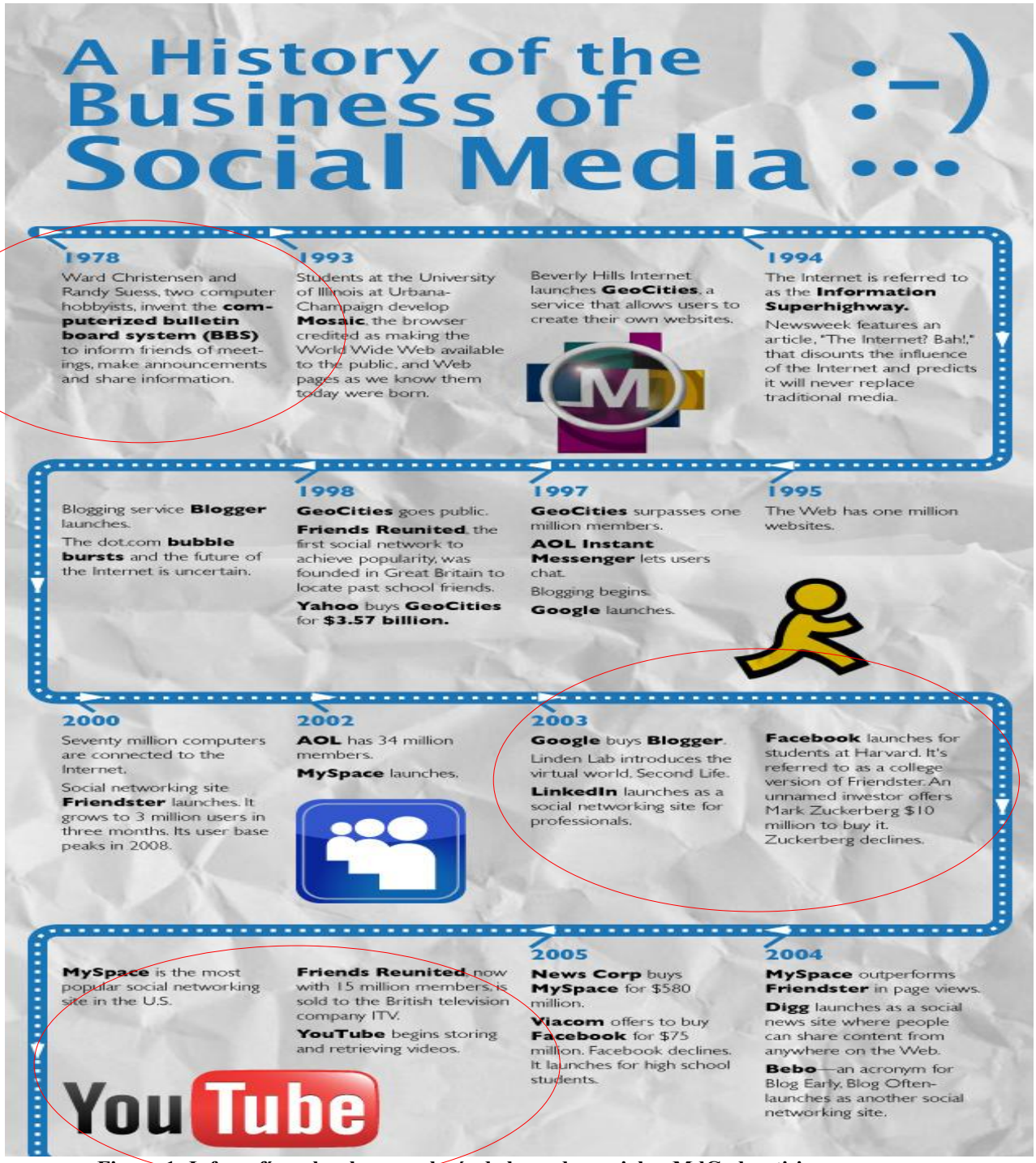

Figura 1: Infografía sobre la cronología de las redes sociales MdGadvertising.
Fuente: http://www.ticbeat.com/socialmedia/triste-estado-privacidad-redes-sociales-infografia/

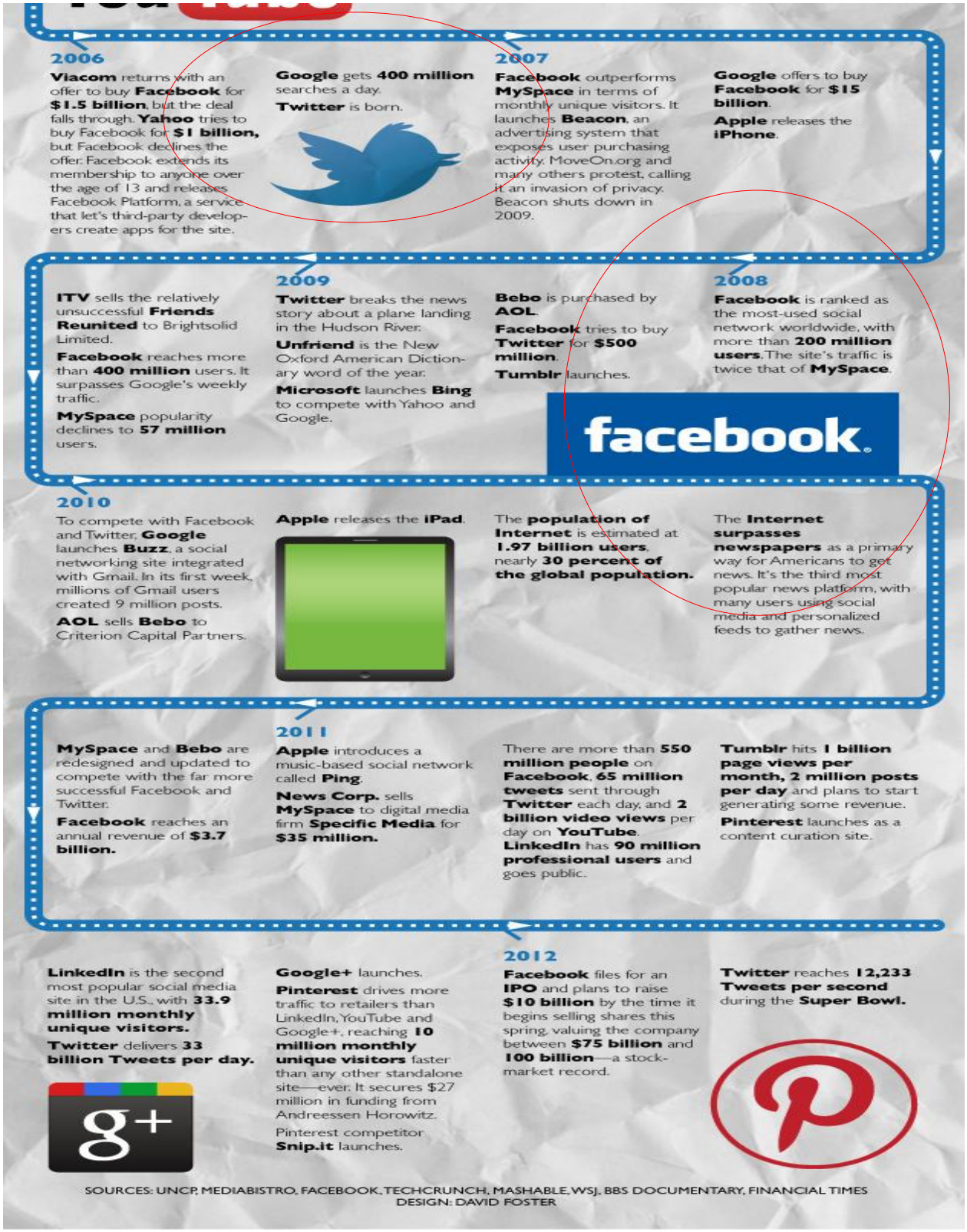

Figura 1: Infografía sobre la cronología de las redes sociales MdGadvertising.
Fuente: http://www.ticbeat.com/socialmedia/triste-estado-privacidad-redes-sociales-infografia/

2.2 Redes sociales versus Privacidad

Sin embargo el desarrollo en nuestra sociedad de estas herramientas sociales conlleva nuevos retos asociados sobre todo los referidos a la protección de la intimidad y de los datos personales , y que en los últimos años es síntoma de preocupación por parte de los profesionales e incluso por parte de los usuarios del vacío existente en cuanto a privacidad y seguridad en las políticas de recogida, retención y uso de los datos personales que volcamos en nuestro perfiles de usuarios de dichas tecnologías. Según (Sánchez Ocaña, 2009)[1] *"las principales redes sociales generalistas se preocupan por mejorar todo lo referente a la privacidad del usuario y permiten gestionar y definir el grado de exposición pública del individuo, pero se echa en falta una legislación ad-hoc que toda red social tenga que suscribir a nivel de privacidad del usuario para poder estar online",* esto nos da la clave de cómo algunos profesionales de los medios sociales ven las sombras legales sobre la utilización de las redes sociales.

En el caso de España desde 2009 se abrió el camino por parte de la Agencia de Protección de Datos (AGPD) respecto a la problemática que presentaban dichas plataformas colaborativas haciendo frente con investigaciones para intentar subsanar algunos aspectos que quedan al descubierto como es el caso de la privacidad con algunas recomendaciones tecnológicas y de seguridad; así como de concienciación en materia de formación a los usuarios para su utilización. Es por esta razón, que desde las administraciones públicas se fomenten nuevos mecanismos que garanticen la seguridad y la credibilidad de acceso de estas nuevas tecnologías; atendiendo a los principales estándares de seguridad en internet también podemos aplicar algunos a la seguridad de las redes sociales, destacando:

- Confidencialidad: Sólo las entidades autorizadas deben tener acceso al contenido de la información.
- Integridad: La información que se publique no sea modificada por ningún tercero salvo por la entidad autorizada.
- Disponibilidad: La administración de estas plataformas deben garantizar la protección del usuario frente a otros.

[1] Artículo de opinión en el periódico Cinco Días del 14 de Octubre de 2009, página 17.

- No repudio: Los participantes del servicio no podrán repudiar sus comunicaciones.

Según Antonio Troncoso Reigada (Director de la Agencia de Protección de Datos) *"la privacidad no sólo trata del respeto a nuestro datos personales sino también del que debemos de tener por la información relativa a los demás"* y en el caso de las redes sociales se ha descubierto una manera de comunicarse y de socializarse de forma distinta que ha cambiado el paradigma de la privacidad y con ello los conceptos que se llevan asociados como la intimidad o la confidencialidad, que no son sinónimos del concepto de privacidad. La confidencialidad es la *"cualidad de los datos e informaciones reservados o secretos por el que empresas o entidades deben garantizar que esa información esté protegida y no se transmita a terceros"* (Vela Sánchez-Merlo, 2008) y no se podrá hacer un uso indebido de esos datos en ningún ámbito.

En el caso de Internet son las entidades las que deben de garantizar la seguridad informática de la información con el objetivo de que nadie pueda acceder a esta información confidencial entre la que podemos encontrar (nombres, direcciones, actividades familiares o personales, datos bancarios) y adquirir el compromiso de almacenar y recoger ,es decir , proteger todos aquellos datos que están vinculados a la vida privada de tal manera que si los administradores de las redes sociales protegen la confidencialidad de nuestros datos estarán salvaguardando la privacidad de las personas, a esto se le denomina políticas de privacidad. Mientras el término intimidad suele dar lugar a confusiones y normalmente lo identificamos con privacidad, en cambio la intimidad es el conjunto de pensamientos, ideologías o sentimientos que cada individuo posee y que forman parte de nuestra privacidad, no viceversa. La intimidad puede no ser compartida ni en nuestra vida física sin embargo la vida privada si la podemos compartir con otros, es lo que ocurre en las redes sociales donde hacemos participes al resto de personas de nuestra faceta de más privada (acontecimientos o situaciones que afectan a nuestro ámbito personal o familiar, etc.) por este motivo muchos individuos de nuestro entorno que no forman parte de estas plataformas vean que su privacidad no esté protegida y se vea afectada por una serie de daños que no se ven amparados por la falta de protección jurídica con la que poder garantizarla, además de desconocerse algunos aspectos de naturaleza jurídica para determinar las obligaciones y

responsabilidades legales de los prestadores de servicios respecto a la privacidad y la protección de datos de los usuarios.

Respecto a las políticas de privacidad, el Instituto Nacional de Tecnologías de la Comunicación en España publica en su sede web (www.inteco.es) una serie de guías para la configuración de la privacidad de gran utilidad para los usuarios de las top 10 redes sociales más populares en nuestro país. A continuación mostramos algunos puntos relevantes de la **política de uso de datos actual de Facebook**, sobre los datos personales que recogen y del uso que se le da en dicha plataforma:

I. Qué información recibimos y cómo se utiliza

Información que recibimos sobre ti

Recibimos diferentes tipos de información sobre ti, como:

Tu información

Se trata de la información necesaria para registrarte en el sitio, así como la que decides compartir.

- **Información de registro**: Cuando te registras en Facebook, te pedimos que introduzcas tu nombre, dirección de correo electrónico, fecha de nacimiento y sexo.

- **Información que decides compartir**: Tu información también incluye todo aquello que compartes en Facebook, como tus actualizaciones de estado, las fotos que subes o los comentarios que haces en la historia de un amigo.

También incluye la información que decides compartir al realizar una acción, por ejemplo cuando añades un amigo, indicas que te gusta una página o sitio web, añades un lugar a tu historia, usas nuestra herramienta de importación de contactos o bien registras que tienes una relación con alguien.

Tu nombre, fotos del perfil, fotos de portada, sexo, redes, nombre de usuario e identificador de usuario se tratan del mismo modo que la información que decides hacer pública.

Tu fecha de nacimiento nos permite hacer cosas como mostrarte anuncios y contenido adecuado para tu edad.

Información que otras personas comparten sobre ti

Recibimos información sobre ti de tus amigos y de otras personas, por ejemplo, cuando suben tu información de contacto, publican una foto tuya, te etiquetan en una foto o en una actualización de estado, en un lugar o cuando te añaden a un grupo.

Cuando la gente usa Facebook, puede almacenar y compartir información sobre ti y otras personas que tienen como amigos, como cuando suben y gestionan sus invitaciones y contactos.

Otra información que recibimos sobre ti

También recibimos otros tipos de información sobre ti:

- Recibimos información sobre ti cada vez que interactúas con Facebook, por ejemplo, cuando consultas la biografía de otra persona, envías o recibes un mensaje, buscas un amigo o una página, haces clic, consultas o interactúas de otro modo con cosas, utilizas una aplicación para móviles de Facebook, compras créditos de Facebook o compras otras cosas a través de Facebook.
- Cuando publicas cosas como fotos o vídeos en Facebook podemos recibir información adicional (o metadatos) como la hora, la fecha y el lugar en el que tomaste la foto o el vídeo.
- Recibimos la información del ordenador, teléfono móvil o dispositivo que utilizas para acceder a Facebook, incluso si varios usuarios inician sesión desde el mismo dispositivo. Esta información puede incluir tu dirección IP y otra información relativa, por ejemplo, a tu servicio de internet, tu ubicación, el tipo de navegador que utilizas (incluidos los identificadores) o las páginas que visitas. Por ejemplo, podemos obtener tus coordenadas GPS u otros datos de ubicación de modo que podamos decirte si tienes cerca a alguno de tus amigos.
- Recibimos datos cada vez que visitas un juego, una aplicación o un sitio web que utiliza la plataforma de Facebook, cada vez que visitas un sitio con una función de Facebook (como un plug-in social) y, a veces, a través de cookies. Esta información puede incluir la fecha y la hora en que has visitado el sitio, la dirección web o URL en la que estás, información técnica sobre la dirección IP, el navegador y el sistema operativo que utilizas y, si has iniciado sesión en Facebook, tu identificador de usuario.
- Algunas veces obtenemos datos de nuestros socios publicitarios, clientes u otras terceras partes que nos ayudan (a nosotros o a ellos) a ofrecerte anuncios mejores, a interpretar la actividad que se desarrolla en línea y, en general, a mejorar Facebook. Por ejemplo, un anunciante podría facilitarnos información sobre ti (como cuál ha sido la respuesta ante un anuncio publicado en Facebook o en otro sitio) para medir la eficacia de los anuncios y mejorar su calidad.

> Nosotros recopilamos datos a partir de la información que ya tenemos sobre ti y sobre tus amigos. Por ejemplo, podemos recopilar datos sobre ti para saber qué amistades te deberíamos mostrar en tu sección de noticias o qué amistades podemos sugerirte que etiquetes en las fotos que publicas. Podríamos unir la ciudad donde te encuentras con información de GPS u otro tipo de información de ubicación que tengamos sobre ti, por ejemplo, para contarte, a ti y a tus amigos, cosas sobre otras personas o eventos que se estén celebrando cerca, o para presentarte ofertas que podrían interesarte. También podemos recopilar datos sobre ti para mostrarte anuncios que puedan interesarte.

2.3 Tipos de redes sociales

Existe una gran diversidad de redes sociales en Internet. Podemos atenernos a cuatro criterios para clasificarlas. El primero y más general, es el grado de especialización. Algunas redes no tienen una finalidad concreta y de este modo aglomeran a una gran masa de gente, ideal para darle fuerza a una red social. Otras tienden a unir personas con aficiones comunes, como la música o los videojuegos, o ayudan a los usuarios a generar relaciones profesionales. También podríamos clasificarlas según su contenido. Observamos que hay redes sociales que se centran en las relaciones entre las personas, muy distintas de las que presentan contenidos delegando los usuarios a un segundo plano, y por último las que relacionan entidades inanimadas, como marcas o incluso difuntos. La tercera clasificación que estudiaremos se basa en la importancia de la localización geográfica**,** ya que algunas webs varían según la cercanía geográfica entre usuarios o entre los usuarios y otros elementos. Y por último, cabe destacar que no algunas redes utilizan plataformas diferentes del web. Es el caso de los llamados *metaversos*, como Second Life, en los que los usuarios se relacionan del mismo modo que en las redes sociales del web, pero utilizando una base técnica diferente. A continuación estudiaremos en detalle la comentada clasificación: **Horizontales / Verticales.**

- **Redes sociales Horizontales**

No tienen una temática definida y están dirigidas a todos los usuarios. Cualquiera puede registrarse y participar libremente sin un fin definido. Cada usuario elige el objetivo de su participación, aunque suelen centrarse en enviar mensajes, invitar, escribir comentarios y estar en contacto con los miembros de su red. Estas redes en definitiva tratan de reunir a una gran masa de gente que interactúe. Los ejemplos más típicos son Facebook o Twitter.

- **Redes sociales Verticales**

Éstas giran en torno a un eje temático. Su objetivo es el de unir a un grupo de personas interesadas en un tema definido. En función de su especialización, podemos clasificar a su vez las redes sociales verticales en:

- ✓ **Redes sociales Verticales Profesionales**

Han sido diseñadas para generar relaciones profesionales y permitir un intercambio de información, y promocionar los distintos usuarios y empresas. Los ejemplos más representativos son Xing y LinkedIn.

Existe una gran diversidad de redes sociales en Internet. Podemos atenernos a cuatro criterios para clasificarlas. El primero y más general, es el grado de especialización. Algunas redes no tienen una finalidad concreta y de este modo aglomeran a una gran masa de gente, ideal para darle fuerza a una red social. Otras tienden a unir personas con aficiones comunes, como la música o los videojuegos, o ayudan a los usuarios a generar relaciones profesionales. También podríamos clasificarlas según su contenido. Observamos que hay redes sociales que se centran en las relaciones entre las personas, muy distintas de las que presentan contenidos delegando los usuarios a un segundo plano, y por último las que relacionan entidades inanimadas, como marcas o incluso difuntos.

La última clasificación que analizaremos se basa en la importancia de la localización geográfica**,** ya que algunas webs varían según la cercanía geográfica entre usuarios o entre los usuarios y otros elementos.

Localización geográfica

- ✓ **Redes sociales Verticales de Ocio**

Unen a gente con aficiones comunes, como el deporte, videojuegos, música, etc. Los ejemplos más representativos son Dogster, Last.FM y Moterus.

- ✓ **Redes sociales Verticales Mixtas**

Ofrecen a usuarios y empresas un entorno específico para desarrollar actividades tanto profesionales como personales. Suelen incluir una agenda online o un buscador de servicios cercanos. Ejemplos de este tipo son PideCita y 11870.

Por el contenido

- ✓ **Redes sociales Humanas**

Son aquellas que se centran en las relaciones entre personas uniendo individuos según su perfil social y en función de sus gustos, aficiones, lugares de trabajo, viajes y actividades. Ejemplos de este tipo de redes los encontramos en Youare y Tuenti.

- ✓ **Redes sociales de Contenidos**

En este caso se relacionan los perfiles a través de contenido publicado por los usuarios. Normalmente se trata de fotos, música o videos. Ejemplos más significativos son Flickr, Bebo, Friendster y FileRide.

- ✓ **Redes sociales de Inertes**

Suponen un enfoque novedoso en lo que a las redes sociales se refiere. Pueden unir marcas comerciales, lugares u objetos inanimados (como vehículos). Entre estas redes sociales destacan las de difuntos, siendo éstos los sujetos principales de la red. El ejemplo más llamativo es Respectance.

Por la importancia de la localización geográfica

- ✓ **Redes sociales Sedentarias**

Este tipo de red social muta en función de las relaciones entre personas, los contenidos compartidos o los eventos creados. Ejemplos de este tipo de redes son: Blogger, Bitacoras.com.

- ✓ **Redes sociales Nómadas**

A las características propias de las redes sociales sedentarias se le suma un nuevo factor de mutación o desarrollo basado en la localización geográfica del sujeto. Este tipo de redes se componen y recomponen a tenor de los sujetos que se hallen geográficamente cerca del lugar en el que se encuentra el usuario, los lugares que haya visitado o aquellos a los que tenga previsto acudir. Los ejemplos más destacados son: Latitud y Skout.

2.4 Derechos potencialmente vulnerables en las redes sociales

La repercusión de las redes sociales y su uso no quedan exentos de recibir constantes ataques por parte de hackers o personas cuya actitud ante estas plataformas es muy diferente al fin de las mismas, muchos colectivos ven afectados algunos principios jurídicos en estos medios sociales. Son un instrumento fácil para llevar a cabo delitos y vulnerar algunos derechos que no se ven exentos de riesgos y ataques malintencionados entre ellos podemos destacar los siguientes:

a) Derecho al Honor

"Es aquel que tiene toda persona a su buena imagen, nombre y reputación, de tal forma que cualquier ciudadano puede exigir que se respete su esfera personal con independencia de las circunstancias particulares" (INTECO, 2009) convirtiéndose en un derecho irrenunciable. Los principales delitos que engloba el derecho al honor son el delito de calumnia y el de injuria. Un delito de **calumnia** es aquel en el que la persona que acusa a otra de haber cometido un delito resultando que tal acusación es

falsa. Tanto el delito como la persona a la que se le imputa su comisión han de estar determinados. Una persona acusada si logra que los hechos del delito de calumnia que se le imputan sobre la persona calumniada sean ciertos, quedará exenta de toda responsabilidad penal.

En el caso de la **injuria** es aquella expresión que lesiona la dignidad de una persona perjudicando su reputación o atentando contra su propia estima. Cualquier persona anónima o conocida en las redes sociales puede atribuir unos hechos, ejercer juicios de valor sobre ella pero las únicas que están tipificadas y que son constitutivas de delito son las injurias consideradas de carácter grave. Este tipo de lesiones es frecuente en algunas redes sociales sobre todo en perfiles públicos de políticos y personajes de proyección social como presentadores de televisión, artistas, deportistas, etc.

En estas plataformas es muy sencillo llevar a cabo delitos o ataques que atenten contra el honor de una persona, y con un simple clic en el muro de una persona se puede publicar un contenido ofensivo de carácter delictivo con el fin de dañar la reputación de una persona.

En el Código Penal estos delitos están tipificados y por tanto amparados por la ley. Aparentemente en las redes sociales conocemos las identidades de los usuarios no así en otros medios en la red donde los usuarios suelen utilizar y firmar con un pseudónimo. Por tanto, la ley podría investigar con mayor facilidad a los autores de las injurias y calumnias, a no ser que hayan utilizado datos falsos, lo cual está prohibido en las redes sociales pero en muchas ocasiones son numerosos los usuarios que emplean estas tácticas para cometer delitos en la red social.

b) Derecho a la Intimidad Personal y Familiar

El derecho a la intimidad personal y familiar, tiene por objeto la protección de la esfera más intima de la persona, también vinculado con la protección de la divinidad de la persona. Así se define en el artículo 18 de la Constitución Española de 1978, donde se señala que "*exigir de los demás el respeto de un ámbito exclusivo que incumbe solamente al individuo, que es resguardo de sus posesiones privadas, de sus propios*

gustos y de aquellas conductas o actitudes personalísimas que no está dispuesto a exhibir, y en el que no caben legítimamente las intromisiones externas."

Respecto a las redes sociales que es el tema que nos concierne en este trabajo no son sitios que ofrezcan exclusividad, ya que el número de personas en línea e interconectadas va más allá de lo meramente exclusivo pero si el contenido informativo que incluye sí puede ser privado, y ahí es donde cada individuo será responsable de todo lo que publique así como de todos los comentarios, opiniones o mensajes que sus amigos en la plataforma publiquen. Por todo ello, y para evitar posibles situaciones de riesgos y proteger la intimidad los individuos debemos de tener en cuenta algunos consejos desde el primer momento que nos registramos como usuarios; debemos ser conscientes de la exposición que vamos a hacer sobre nuestras actitudes personales ya que se va a publicar información de carácter susceptible y sensible desde el inicio, también debemos ser precavidos a la hora de hacer un seguimiento de nuestras publicaciones, datos e imágenes porque nuestra privacidad se puede ver afectada así como la de terceros. Las redes sociales son potentes herramientas que controlan el alcance de nuestros datos y con ello el de nuestra privacidad; son capaces de intercambiar, procesar y de analizar la información e incluso indexar los perfiles de los usuarios con información del contacto poniendo en riesgo la privacidad y la de nuestros amigos complicándose la posible eliminación de cualquier rastro sobre nuestros datos personales.

c) Derecho a la Propia Imagen

El derecho a la propia imagen atribuye a cada individuo de la potestad para disponer de su imagen física impidiendo su difusión salvo que medie su propio consentimiento.

Las redes sociales permiten nuevas formas de reproducir la imagen de una persona y hacerla pública de forma instantánea, incluso sin que ésta se dé cuenta. Normalmente, los usuarios de redes sociales no solemos pedir consentimiento a los terceros sobre las publicaciones de imágenes en nuestros perfiles o muros sobre momentos o acontecimientos íntimos provocando que un usuario que quiera salvaguardar su imagen encuentre una foto suya circulando por las redes sociales sin el permiso necesario, e incluso a veces vamos más allá etiquetando las fotos con datos personales (nombres, apellidos e incluso el sitio donde fueron tomadas las imágenes) , en la mayoría de las redes sociales la persona que ha subido una imagen es la responsable de difundir,

salvaguardar y la única que puede borrar el etiquetado de un individuo que aparezca aunque su imagen ya ha sido expuesta públicamente y podría haber reproducciones extendidas por toda la red. Actualmente, las redes sociales permiten denunciar imágenes donde aparecen usuarios que han sido etiquetados sin su consentimiento.

En nuestro país, estos derechos se encuentran amparados en la Ley Orgánica 1 /1982, de 5 Mayo de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen basada en la disposición constitucional del Art.18.1 de la Constitución Española, pero no se hace mención expresa al uso de la redes sociales de manera que los derechos de los usuarios pueden quedar sin una defensa legal efectiva. También es necesario mencionar a los usuarios menores de edad, que son un grupo de población mayoritariamente muy activo en las redes sociales y a los intereses que se defienden en la legislación que es más elevado que el resto sobre la protección de sus derechos en estas plataformas y de la que es necesaria la intervención de los padre o de los tutores legales debiendo notificar dicha publicación a la Fiscalía de Menores (artículo 3.2) aunque esta ley no se respeta en ninguna de las plataformas, teniendo en cuenta que la edad mínima para participar es de 13 a 14 años.

d) Derecho a la Libertad

En España, el derecho a la libertad está amparado en **Código Penal en el Título VI** donde se hace mención a *proteger la libertad de los individuos, que se concreta en dos dimensiones: la libertad de obrar y la libertad de querer. Siempre que un particular prive a un individuo de cualquiera de estas dos libertades, estará incurriendo en un delito*. Dentro de los delitos contra la libertad nos podemos encontrar cuatro tipos diferentes que atentan contra esta: la detención ilegal, el secuestro, la amenaza y la coacción.

En relación a las redes sociales respecto a la detección ilegal o secuestro es muy complicado que se llegue acometer delitos de esta índole, aunque son herramientas que pueden facilitar a los medios legales y policiales información valiosa sobre un individuo concreto (localización, hábitos, intereses, contactos, etc.). Más frecuentes son los **delitos de amenazas,** un sujeto advierte o anuncia a un individuo incurriendo en el miedo, acoso con el propósito de infundirle miedo o extorsión a él mismo e incluso al entorno

vinculado con él, este tipo de lesiones son constitutivas de otros delitos como homicidio, lesiones, aborto, torturas, contra la libertad, la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio, etc. Este tipo de amenazas en las redes sociales pueden generar en un individuo intimidación e incluso atentado contra la propia seguridad del individuo; en estos casos los expertos en seguridad en servicios Web y juristas recomiendan denunciar para que se tomen las **medidas cautelares urgentes** necesarias para proteger sus derechos frente a los ataques malintencionados como usuarios en las redes sociales. En cuanto al **delito de coacción** consiste en la acción de impedir o de obligar a una persona a hacer lo que no desea con **violencia física** o **psicológica**. En el caso de las redes sociales, el delito de coacción se puede cometer mediante la publicación de un contenido en el muro de un perfil o un mensaje privado amenazando a un usuario.

e) Derecho a la Libertad de Expresión

Las redes sociales son plataformas que permiten a los usuarios generar un perfil público en el que plasmar datos e información de carácter personal, cualquier usuario puede publicar lo que desee aunque las propias redes sociales someten los contenidos a un cierto control. Este tipo de manifestaciones en las que el usuario publica contenido de cualquier índole hace que se violen los derechos de otros individuos. El entramado de una red social es muy complicado de gestionar, sobre todo lo que respecta a los contenidos o publicaciones que hace cada uno de los miembros de estas redes, en la constante actualización y protección de los derechos de los usuarios los administradores de las redes sociales están implantando nuevos mecanismos para denunciar abusos de contenidos e imágenes que puedan atentar contra la privacidad y intimidad de un individuo.

Los administradores de las redes sociales se comprometen en sus políticas a configurar correctamente sus canales de comunicación para identificar si los contenidos publicados infringen la ley o no, de manera que se eliminen o se eliminen perfiles que abusen contra cualquier derecho del individuo así como contra cualquier derecho de propiedad intelectual o industrial .La protección de estos derechos que pueden ser vulnerados en las redes sociales entra en conflicto con la libertad de expresión de los individuos en estas mismas plataformas muchos usuarios de estas hacen uso de estos canales como medio de difusión de sus tendencias sexuales, ideologías sociales y políticas como vía

para expresar opiniones, críticas sobre acontecimientos relacionados con nuestra propia vida personal o sobre aspectos relacionados con aspectos de gran envergadura social , aunque nos podamos encontrar con grandes barreras legales para ello.

f) Derecho a la Propiedad Intelectual

Otro de los derechos que sufre gran vulnerabilidad en las redes sociales es la propiedad intelectual; en estas plataformas existe contenido protegido mediante propiedad intelectual e industrial. Cada vez más se esta produciendo un aumento en el número de contenidos protegidos que son difundidos, compartidos e utilizados a través e las redes sociales, en España dicha protección se ve amparada en la Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril donde "*se refleja que los autores de las obras tienen derechos en exclusiva sobre los mismos, lo que supone que cualquier tratamiento , reproducción, puesta disposición o transmisión de la obra deberá ser realizada con la autorización con la autorización de los titulares de los derechos*". Respecto a las posibles vulneraciones de propiedad intelectual en las redes sociales, los derechos de propiedad intelectual y la integridad de los autores se ponen en entredicho ya que no se hace mención en ninguna de las cláusulas de las condiciones generales de las políticas de privacidad por lo que queda un vacío muy aparente respecto a este derecho.

Las redes sociales están publicando contenidos gráficos, musicales, audiovisuales, etc sin autorización del titular. Es decir, se están reproduciendo y comunicando de forma pública obras protegidas mediante propiedad intelectual cuyos derechos tienen en exclusividad el autor o autores a caso que ellos mismos cedan expresamente dichos derechos de divulgación. Las propias plataformas son conscientes de la vulneración y distribución de materiales que no están exentos de derechos legales, de ahí que muchas hayan decidido colaborar contra la distribución de materiales no autorizados por sus autores y proveer de mecanismos automáticos para que los propios usuarios de la red social regulen los contenidos y denuncien los contenidos que nos son propios y que atenten contra los derechos de los autores o de terceros. Cuando nosotros publicamos contenidos protegidos por la ley y lo hacemos mediante canales de alcance público como es el caso de las redes sociales, corremos el riesgo de que puedan ser copiados por

parte de terceros en esa misma red social u en otras pudiéndose difundirse rápidamente el contenido que esta bajo tutela del autor.

También debemos mencionar otro aspecto muy recurrente que se produce en las redes sociales y es la transformación de contenidos; normalmente los usuarios extraemos citas, contenidos de obras y documentos que tienen derechos de autor y los publicamos en las redes sociales y es la propia ley la que contempla que no es necesario tener el permiso del autor para publicarlo; esto desencadena en un paradigma entre la legislación vigente y el ámbito tecnológico. Establecer un control fiable y consecuente por parte de las redes sociales a las obras y contenidos con derechos de autor es muy difícil, para eso sería necesario un cambio en el tratamiento de diversos aspectos en la elaboración de las leyes actuales y venideras, los legisladores además deben de tener en cuenta que muchos usuarios de las redes sociales ya no son simples receptores de contenidos sino que cada vez más son creadores de nuevos contenidos, informaciones , vídeos , imágenes que son subidas a estas plataformas sociales como es el caso de Deviantart que realiza creaciones gráficas, Flickr (fotografías) o MySpace red social donde los usuarios cuelgan todo tipo de música. Por ello, los usuarios e incluso los propios administradores de redes sociales necesitan saber que ocurrirá con los contenidos de los usuarios una vez subidas nuestras obras a una plataforma como MySpace o Tuenti, para evitar posibles abusos de los mismos.

En redes sociales como Tuenti o Facebook, el responsable del contenido siempre será el usuario, aunque cualquier tipo de contenido quedará almacenado aunque el usuario lo elimine o cuando éste cancele su cuenta en la red social. Al igual que las dos anteriores redes sociales, MySpace tiene la cesión del contenido mientras el usuario utilice el servicio impidiéndosele la sub-explotación comercial de dichos contenidos, llevando a cabo una política de actuación correcta en cuanto a la publicación de los contenidos aportados por los usuarios.

g) Derecho de Propiedad Industrial

En lo referente a la propiedad industrial en las redes sociales se ve afectada la marca o el logotipo con signo distintivo. Las redes sociales son plataformas a través de las cuales se puede obtener un beneficio económico que deriva de las estrategias de marketing y

publicidad que llevan a cabo algunas empresas para lograr una mayor proyección empresarial pero en lo que afecta al derecho del usuario este tiene la capacidad de publicitar y ser receptor de anuncios de forma masiva.

Las redes sociales cuentan con bases de datos potentes con usuarios potenciales a los que en muchas ocasiones se les invade con numerosos anuncios publicitarios, por eso los administradores de las redes sociales junto con los legisladores están intentando autorregular este tipo de prácticas publicitarias que en cierto modo vulneran en algunas ocasiones la seguridad de los usuarios e incluso muchas marcas pueden ver dañada su imagen simplemente con que cualquier usuario emplee el logo de una marca para desprestigiarla sin justificación; como por ejemplo que los McPollo´s de la marca McDonald´s pueden transmitir la gripe aviar o que un usuario se identifique con una marca en su perfil se estarían violando los derechos de la marca; también la Ley ampara y protege a todas aquellas creaciones intelectuales, artísticas e industriales que solventen problemas tecnológicos o relacionados con el diseño o tengan una repercusión en el ámbito económico.

2.5 Datos privados publicados y vulnerables en las redes sociales

Las redes sociales como servicios Web comunitarios se convierten en una fuente de información muy exhaustiva y jugosa para la manipulación de datos de terceros, normalmente las personas en su vida diaria no hacemos saber a otros aspectos relacionados con nuestra vida cotidiana para poder salvaguardar la privacidad de nuestro entorno. Sin embargo las redes sociales han conseguido encontrar ese punto embaucador para atraer a distintos perfiles donde los usuarios publican contenidos, muchos de ellos relacionados con acontecimientos de la vida privada o relacionados con la propia intimidad del usuario, otras veces son terceros los que comparten y difunden contenidos sobre nuestra propia persona en su mayoría sin consentimiento expreso en muros o mediante tweets rompiendo así las barreras entre lo que es público y privado. Las personas perdemos la privacidad cuando nos exponemos ante los demás y nuestros comentarios, opiniones e incluso movimientos físicos que sirven de atención para otros aunque sea sin que nos percatemos de las acciones de los otros eso es lo que ocurre en las redes sociales. Por ello, es necesario presentar y abordar cuáles de esos

datos que se publican en las redes sociales son sensibles y afectan al equilibrio entre la privacidad perfecta y la total pérdida de privacidad.

a) Vida sexual, amorosa

Como mencionamos anteriormente, a través de las redes sociales y de muchos perfiles de usuarios podemos conocer la vida sexual y amorosa de las personas mediante cambios de estado, mensajes en el muro o fotos, nuevas incorporaciones a la red social. En algunas redes sociales, la propia configuración de nuestra cuenta nos motiva a añadir algunos datos personales relacionados con nuestra situación sentimental o sexual; por ejemplo en Facebook podemos agregar datos en campos como "Me interesan" ahí estaríamos dando a conocer nuestra tendencia o gustos sexuales o en "Busco" o "situación sentimental ", damos a conocer abiertamente nuestro entorno a terceros tanto a los que tenemos agregados a nuestro perfil como a usuarios desconocidos, ofrecemos pistas muy fiables sobre nuestra privacidad e intimidad y eso puede ser decisivo a la hora de que valoren nuestra reputación o incluso favorecer a situaciones de riesgo para la integridad física o psicológica de un usuario y su entorno más cercano.

Recientemente apareció el caso de Olvido Hormigos, concejala del Ayuntamiento de Yébenes (Toledo) con la publicación de un vídeo erótico en la red social de Youtube difundido entre sus conocidos a través de tecnologías interactivas móviles (Whatsapp) hasta llegar a dicha red social, donde millones de usuarios podían descargar el vídeo y conocer el contenido explicito del vídeo , de este modo se puede ver como una parte tan importante de su privacidad como es la vida sexual y amorosa se vio afectada sin su consentimiento[2]. También se conocen casos que han provocado delitos más graves como asesinatos, el caso que más sorprendió a la opinión pública fue el de Brian Lewis que asesinó a su esposa Hayley Jones en EEUU por un ataque de celos cuando esta cambió su "situación sentimental "en su perfil de Facebook de casada a soltera; su marido no soportaba según declaró posteriormente la dedicación casi exclusiva de su vida a la red social[3].

[2] http://www.elmundo.es/elmundo/2012/09/06/espana/1346918615.html

[3] http://www.geekets.com/2009/09/esposo-mata-a-su-mujer-por-cambiar-de-estado-en-faceebook/

El control y el espionaje que puede ejercer un usuario sobre nuestros perfiles y sobre todo sobre las informaciones y contenidos que difundimos en la red puede ser causante de una invasión en nuestra privacidad e intimidad de la que probablemente sea muy difícil de poder salir pero para ello podemos enfrentarnos a ello con la imposición de medidas personales como por los mecanismos de seguridad que facilitan las redes sociales aunque en muchas de ellas sean precarios, debemos de ser conscientes de que la vida privada de una persona se encuentra más expuesta ahora que antes, hacemos público detalles que antes solo quedaban en nuestro entorno y ahora quedan expuestos a un golpe de clic. A continuación mostramos un ejemplo en la Figura 3.

Figura 2 : Ejemplo de información básica sobre vida sexual o amorosa en Facebook

b) Entorno Familiar

El entorno de las redes sociales ha cambiado el concepto de privacidad y los aspectos personales que en la vida cotidiana apenas lográbamos manifestar públicamente lo han conseguido las redes sociales. En nuestros perfiles sociales tenemos agregados numerosos contacto muchos de ellos con los que no tenemos un contacto desde el colegio, la universidad o simplemente más allá de un simple día que los conocimos y nos intercambiamos las cuentas de la redes sociales ; eso conlleva a que muchas aspectos que muestran nuestra vida diaria sean puestos en conocimiento a otras personas con las que apenas tenemos un trato cercano, mostrando nuestra identidad a terceros a través de fotos de perfil, videos, textos,etc. Informamos sobre nuestro día a día, si hay algún cambio de estado en nuestra vida, trabajo, o simplemente que estamos haciendo y donde. A continuación mostramos un ejemplo en la Figura 4.

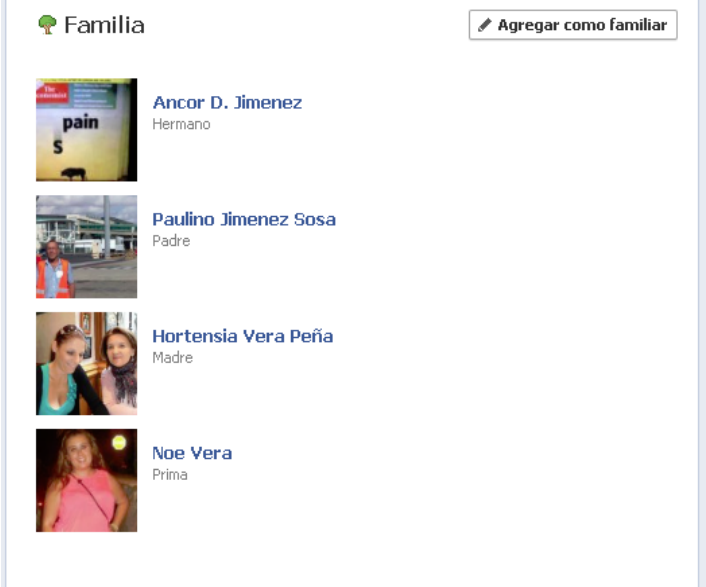

Figura 3 : Información básica de un usuario sobre su vida familiar en Facebook

Datos privados publicados voluntariamente que afectan al usuario

Es necesario distinguir entre los datos que corren riesgos y que son publicados con el expreso consentimiento del usuario a aquellos que son inherentes al uso de estas plataformas.

Datos privados publicados voluntariamente que provocan riesgos a terceros

Es frecuente por parte de muchos usuarios comunicar cambios de estados o situaciones relacionadas con la vida privada como por ejemplo el embarazo, nacimiento de un bebé e incluso publicar imágenes de las ecografías o de los niños en el entorno familiar, acontecimientos o celebraciones con familiares.

A continuación mostramos un ejemplo de lo mencionado anteriormente, observamos cómo un usuario publica en su muro la ecografía de un feto, en esta imagen cualquier tercero puede observar datos sensibles que pueden afectar a la privacidad de un individuo pero son imágenes publicadas voluntariamente por el usuario. A continuación mostramos un ejemplo en la Figura 5.

Figura 4 : Fotografía con datos privados de un tercero en Facebook

Una utilización responsable por parte de los miembros de una red social resulta fundamental para evitar gran cantidad de problemas relacionados con la privacidad. Es el caso de fotos de acontecimientos familiares o sociales que difundimos a través de estas plataformas donde aparecen terceros a los que hemos etiquetado con sus datos personales y donde la propia plataforma localiza por defecto en dicha fotografía exponiéndonos a que cualquier usuario puede identificar a golpe de clic la identidad de una persona como se muestra en la imagen posterior. A continuación mostramos un ejemplo en la Figura 6.

Figura 5 : Fotografía con datos privados que revela la identidad de un tercero en Facebook

c) Entorno Laboral

La inmersión de las redes sociales también ha salpicado al entorno laboral, en el caso de España un 74% de los empleados hace uso de las redes sociales en su trabajo (véase la figura 7). En muchas ocasiones en las organizaciones su uso es necesario, en otras supone un "castigo"para el trabajador. Los profesionales utilizan las **redes sociales** para encontrar a personas, información o conocimientos, para colaborar e intercambiar **contenidos** que amplían sus relaciones personales y profesionales.

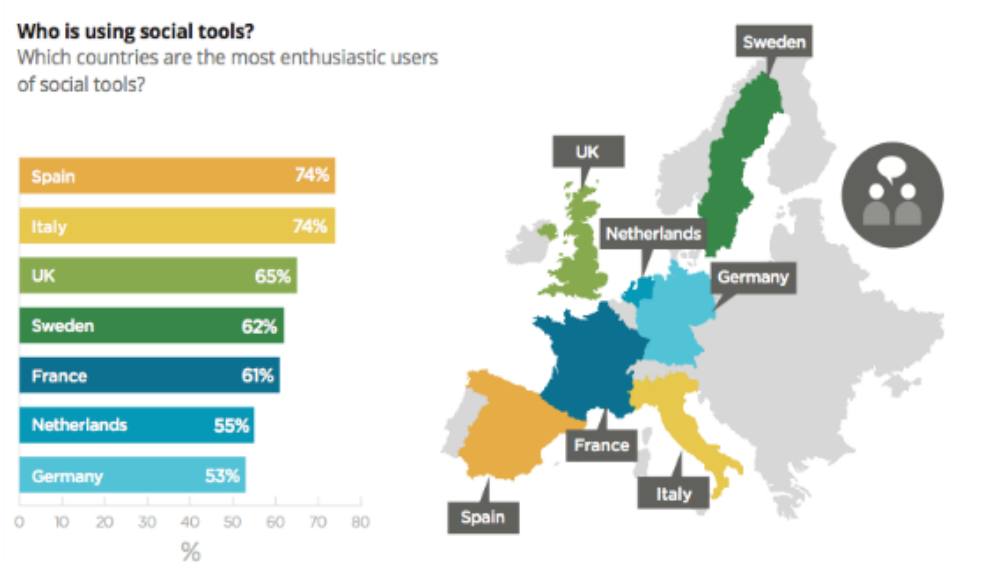

Figura 6: : Gráfico con datos estadísticos sobre el uso en el entorno laboral de las redes sociales por países.

Fuente: http://www.abinternet.es/redes-sociales-entorno-laboral-caso-espana/

Pero también dejan al descubierto aspectos relacionados con su privacidad y que pueden terminar en el despido del trabajador; la publicación de contenidos relacionados con el entorno laboral en nuestro perfil puede tener consecuencias negativas por ello es necesario ser conscientes de que hay ciertos aspectos de las **redes sociales** que generalmente se omiten de una forma u otra, y que pueden perjudicarnos sobre todo si no tenemos una sensación de privacidad y no tomamos precaución para prevenir de un peligro a nuestra reputación dentro de la empresa u organización.

Para eso, cualquier usuario debe tomar previsión para proteger su entorno laboral y llevar a cabo una serie de medidas que le aseguren cierto grado de privacidad, como:

- Evitar publicar cuando nos registramos en una red social nuestra dirección de correo de la empresa, mejor una dirección personal.
- Intentar evitar hacer comentarios en nuestros perfiles sobre la empresa o manifestaciones sobre nuestro estado de ánimo en el trabajo.
- Evitar mezclar los contactos de trabajo con nuestros amigos personales.
- Prohibir que nadie vea nuestro perfil o información personal sin nuestro consentimiento.

Actualmente, la implantación de las redes sociales en los dispositivos móviles también tiene sus consecuencias en el entorno laboral, como:

- No guardar informaciones comprometidas en nuestro teléfono móvil.
- No guardar contraseñas o claves de sitios Web en el móvil.
- Hacer uso de las funciones de seguridad que faciliten estos dispositivos de forma que se eviten riesgos en la privacidad de un individuo.

Por esa razón, la publicación de datos personales, estados o comentarios relacionados con el entorno laboral puede tener consecuencias negativas no solo para un individuo sino para una empresa en general, por lo que el individuo debe ser consecuente con sus manifestaciones, ya que dichos comentarios pueden extenderse a través de otros sitios Web como foros, blogs, etc., rápidamente y aunque se proceda a su borrado el contenido puede quedar disperso por toda la Red.

A continuación, mostramos algunos ejemplos de la publicación de datos privados que afectan al entorno laboral en las Figuras 8 y 9.

Figura 7 : Comentario en Facebook sobre datos privados del entorno laboral

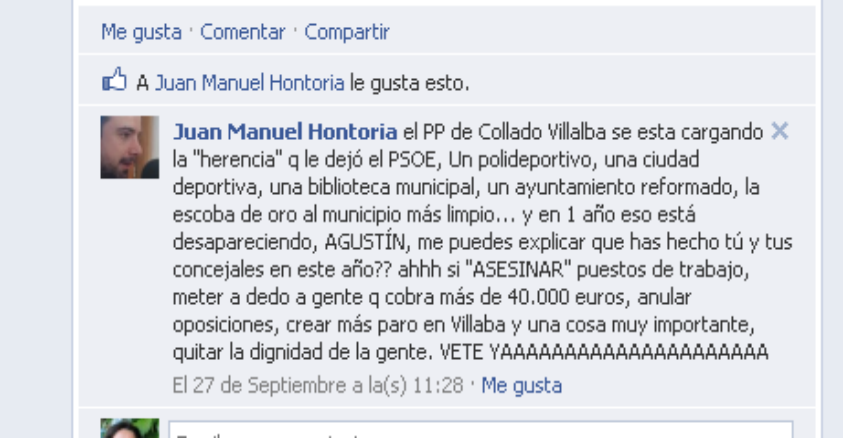

Figura 8 : Opinión política en relación a despidos de trabajadores en Facebook

d) Datos privados de Personajes Públicos

Al igual que las personas que no tenemos una proyección social y vemos como los datos publicados en las redes sociales corren riesgos que garanticen nuestra privacidad, los personajes públicos también comparten y divulgan contenidos con los que deben de tener especial precaución dada la magnitud social que puede alcanzar cualquier estado o información manifiesta a través de las redes sociales. Muchas de las manifestaciones que realizan estos usuarios pueden ocasionar la pérdida de privacidad sobre aspectos que en muchas ocasiones se mantienen en la intimidad personal del individuo y por lo cual se corren riesgos intrínsecos ya que en muchas ocasiones dichos contenidos pueden ser utilizados por terceros para calumniar, injuriar e incluso recibir amenazas contra su persona dada la aceptación o valoración social que se tenga el individuo.

La mayoría de los personajes famosos emplea las redes sociales para poner en conocimiento del gran público su situación profesional, sentimental, familiar o simplemente aspectos privados de su vida más íntima como la publicación de su estado de salud y su evolución en sus muros o mediante tweet.

Los casos más frecuentes que definen este tipo de situaciones son las de los políticos, deportistas y personas relacionadas con la televisión. Desde este punto de vista son muchos los políticos que se han ido integrando a las redes sociales sobre todo cuando se acercan períodos de elecciones crean perfiles en las redes sociales pero lo cierto es que una vez pasados los comicios, pocos son los que se acuerdan de actualizarlos y por

norma general son pocos los que responden a los comentarios de sus usuarios. A pesar de ser los más seguidos, son los que menos interactúan y responden, ni comentan sus actualizaciones.

Algunos casos que han provocado polémica son; el caso de Fernando Autrán, coordinador general de Circulación de Madrid. Que fue destituido por Gallardón por el contenido injurioso en una serie de comentarios vertidos en la red social Twitter[4]. Otros ejemplos sobre publicación de datos sensibles por parte de personajes públicos es el de la compañera sentimental de Francois Hollande, presidente de la república de Francia que publico en su Twitter : "*Simplemente estoy orgullosa de acompañar al nuevo presidente de la República y siempre feliz de compartir la vida con François*", un mensaje con un contenido polémico que levantó las iras entre la clase política francesa dada la situación sentimental del político y que hasta entonces se mantenía como un tema de carácter privado.

Hoy las redes sociales son medios de comunicación más rápidos e interactivos donde las personas somos capaces de poner en conocimiento de los demás los aspectos más privados del individuo y donde los personajes públicos ven un medio de publicitar su imagen y su profesión pero a la vez que se expone un perfil del individuo se corre el riesgo de que terceros publiquen comentarios y opiniones acerca de lo que les acontece y rodea tanto de forma positiva como negativa , es el caso reciente de la cantante española Marta Sánchez que fue injuriada y calumniada en Twitter por unas declaraciones públicas en televisión que provocaron un gran polémica[5].

e) Geolocalización

La geolocalización, es una pieza más del puzzle denominado **'Web 2.0'** (en camino de la Web 3.0 o Web Semántica), un paso lógico en la evolución del concepto 'red social', una plataforma con una utilidad especifica: práctica para quienes les guste ser guiados,

[4] http://www.publico.es/espana/405936/gallardon-destituye-a-un-alto-cargo-por-sus-insultos-en-twitter
[5] http://www.diariocriticocv.com/ciudadanos/marta-sanchez/funcionarios/programa/declaraciones/sara-carbonero/telecinco/que-tiempo-tan-feliz/416302

divertida para aficionados a juegos de rol, poco útil para descubrir sin ayuda de nadie, y sin sentido para quien no entienda.

Los servicios basados en la geolocalización también tienen cabida en las redes sociales por su inmediatez ya que son capaces de dar a conocer en tiempo real la localización geográfica de un individuo o lugar concreto, es decir, tienen utilidad indiscutible tanto para empresas como para usuarios**.** Con respecto a la privacidad, aquí entra en juego el concepto "locational privacy" que consiste en que todo individuo tenga la seguridad para poder moverse en un espacio sin que su situación posicional sea grabada para un fin posterior, a través de la situación geográfica de un individuo o de un determinado momento publicado en una red social se pueden conocer aspectos relacionados con la vida de una persona desde la ideología política(asistencia a mítines, manifestaciones),relaciones con otras personas(acontecimientos en un determinado lugar, hotel, casa), enfermedades (publicar el hospital donde tenemos un tratamiento), e incluso nuestra confesión religiosa (actos y lugares religiosos donde profesamos una religión) son algunos de los contenidos que podemos revelar que atenten contra la privacidad e intimidad de la persona .Por ejemplo, *"las fotos tomadas por muchos teléfonos son sistemáticamente codificadas con etiquetas de latitud y longitud. Cuando los usuarios envían las fotos online a través de servicios como TwitPic, exponen muchos más datos personales de los que se creen."*

Involuntariamente podemos dar información que a primera vista parece inofensiva pero que posteriormente puede implicar peligros importantes de seguridad.

Abordar el tema de la geolocalización implica hacer una **reflexión sobre la privacidad** ahora no solo compartimos fotografías, tenemos una lista pública de quienes son nuestros amigos o familiares, y/o tenemos efecto viral sobre lo que pensamos, vemos o comemos, sino que también nos registramos en el mapa de la aplicación verificando ante los demás que hemos estado ahí. Todas estas maneras de compartir información con los demás, de un modo nunca antes había sido expuesto de forma tan 'abierta' y 'pública' nos hace pensar, en una sociedad exhibicionista pero haciendo una valoración más exhaustiva podríamos hablar de un nuevo concepto de privacidad a través de las

redes sociales y su implantación en dispositivos móviles : la **privacidad 2.0**.[6] Si la comunicación es 2.0, el pensamiento es 2.0, nuestra cultura y modo de vida también lo es, la privacidad, por lógica, también **se traslada a esta nueva dimensión: los límites de lo íntimo y lo público están cambiando y evolucionando**. Hacia dónde y cuál será el significado exacto de privacidad en unos años, son preguntas que el tiempo contestará pero que la geolocalización ha puesto al descubierto. Sin embargo, la implantación del **uso de la geolocalización** debería ir velada por unas bases legales más efectivas que regulasen este tipo de sistemas para diseñar nuevas características de privacidad que controlasen la publicación de datos de localización en redes sociales.

Figura 9 : Fotografía que revela datos privados de una enfermedad y lugar de tratamiento en Facebook.

[6] http://www.tendencias21.net/La-geolocalizacion-de-los-smartphones-amenaza-la-privacidad_a6357.html

Figura 10 : Fotografía que revela datos sensibles una confesión religiosa de un individuo en Facebook.

e) Riesgos sobre la privacidad en Menores de Edad

La gran eclosión de las redes sociales en Internet ha favorecido que no solo personas adultas hagan uso de estas plataformas interactivas sino que los menores también las hayan focalizado como una herramienta de comunicación instantánea capaz de mantener las relaciones personales entre grupos de amigos, la franja de edad de personas que hacen uso ha disminuido notablemente y con ello los riesgos intrínsecos de las redes sociales. Esos riesgos han traspasado el ambiente físico a las redes sociales, que se han convertido en el medio perfecto para reoganizar este tipo de comportamientos que atentan contra la privacidad y la seguridad de los menores.

En España, el **Informe sobre** "**Menores y Redes Sociales" presentado el día 20 de Enero de 2012 en Madrid por la Fundación Telefónica,** afirma que casi el 70% de los menores internautas españoles son usuarios de redes sociales y entre las más populares según este estudio para este grupo de edad destacan: Tuenti (con un 60% de usuarios) , seguido a bastante distancia Facebook(con un 21%) ; y en tercer lugar se

posiciona Windows Live Spaces(con un 14%), seguida de MySpace y Hi5 (con un 12%) .

Por lo que en líneas generales podemos concluir que el uso de redes sociales en este grupo de usuarios es muy intenso y el grado de familiaridad con estas plataformas afecta a todos los aspectos de su vida cotidiana (ocio, estudios, y relaciones). A través de estos sitios Web los menores se comunican, conocen, comparten y divierten por lo que la exposición que se hace de determinados aspectos de su vida son mayores que la de los adultos, lo que conlleva en muchas ocasiones a que su vida privada sea sometida a una serie de riesgos o amenazas, a continuación mostramos un gráfico, donde observamos el índice de preocupación de las principales amenazas en redes sociales que afectan a los menores de edad.

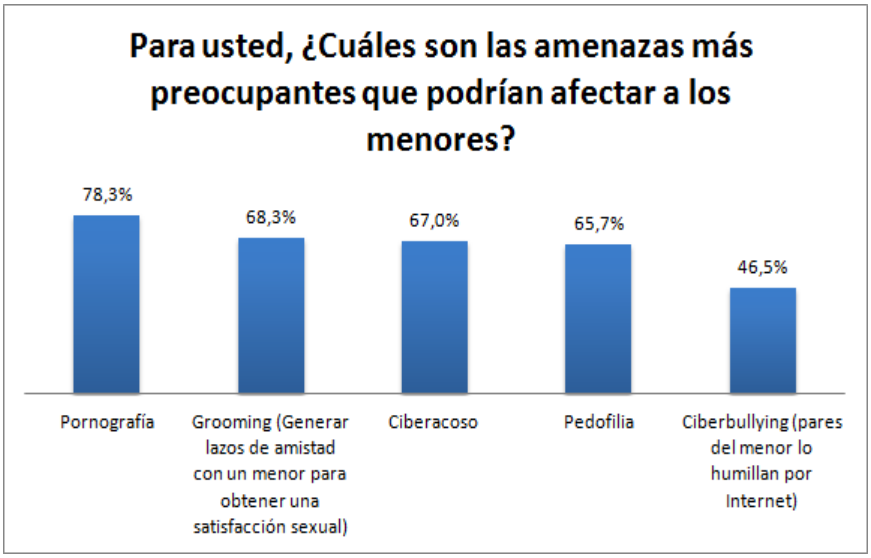

Figura 11 : Gráfico con porcentajes sobre los riesgos que afectan a los menores en redes sociales
Fuente: http://blogs.eset-la.com/laboratorio/2012/06/14/878-adultos-considera-muy-importante-seguridad-menores-internet/

1. Pornografía Infantil

La mayoría de los menores tienen un perfil en Internet, donde cada vez el número de participación es más amplio y donde la edad de incorporación a estas plataformas va disminuyendo considerablemente, en el caso de España la edad minima son 14 años sin embargo muchos adolescentes suplantan sus identidades para poder acceder a estas redes personales y eso a día de hoy no esta controlado por parte de la administración de las redes sociales.

El hecho de cada vez más los menores de edad pasan más tiempo en las redes sociales, los ciberdelincuentes explotan más sus delitos a través de la red. Son conocedores de que las redes sociales son puntos estratégicos para atraer a usuarios y vincular a estos a enlaces maliciosos como páginas webs con contenidos pornográficos además del spam que se ha convertido en una importante fuente para cometer este tipo de delitos.

Las redes sociales no están exentas de su parte de culpabilidad por lo que deberían de establecer en sus políticas de privacidad nuevos mecanismos o tecnologías que impidiesen que niños menores charlasen con desconocidos, colgasen fotos e información personal sin ningún control, la mayoría de redes sociales opera bajo las legislaciones vigentes en Estados Unidos y todas están expuestas a este tipo de delitos. Por esta razón, los administradores de dichas plataformas deben de retirar los contenidos rápidamente que son consistentes de delitos y son denunciados por los usuarios; en el caso de Twitter existe una dirección de correo electrónico donde se pueden denunciar este tipo de delitos (cp@zendesk.twitter.com), en el caso de Facebook hay habilitada una opción que permite denunciar imágenes que incurran en un delito. A continuación mostramos un ejemplo en la Figura 13 de una de las opciones que habilita Facebook para denunciar contenidos e imágenes.

Figura 12 : Opción habilitada por Facebook para denunciar una foto

2. Grooming

Como anteriormente comentábamos, las redes de pedofilia están muy bien organizadas en las redes sociales lo que significa que para los medios policiales es un obstáculo añadido a pesar de contar con herramientas potentes de erradicación de este tipo de delitos que se ven intensificados en los medios tecnológicos; además de la pornografía están apareciendo nuevas amenazas que atentan contra la privacidad de los menores en estos medios sociales, una de estas amenazas que está surgiendo con fuerza es el Grooming, que según el Instituto Nacional de Tecnologías de la Comunicación se

define como *"la acción que tenga por objetivo minar y socavar moral y psicológicamente a una persona, a fin de conseguir su control a nivel emocional*". Este tipo de amenaza se puede llevar a cabo contra cualquier persona pero se considera de carácter grave cuando las coacciones y presiones emocionales van en contra de un menor, con el objetivo de obtener cualquier tipo de favor sexual. En los medios sociales se ofrecen muchas estrategias para entrar en contacto con un menor , una de ellas es que el pedófilo entre en contacto con un menor simulando que él es menor de edad también, consiguiendo datos personales e imágenes del menor con las que luego puede coaccionar o amenazar publicándolo o enviando a todos los contactos con el objetivo de conseguir su fin.

Este tipo de actividades que conforman el "grooming", se ve tipificada en la **Ley Orgánica 10/1995, 23 de noviembre, del Código Penal** que califica como un delito de acoso sexual según lo estipulado en el **Artículo.184** del Código Penal. "…*El que solicitare favores de naturaleza sexual para sí o para un tercero, en el ámbito de una relación laboral, docente o de prestación de servicios, continuada o habitual, y con tal comportamiento provocare a la víctima una situación objetiva y gravemente intimidatoria, hostil o humillante, será castigado, como autor de acoso sexual, con la pena de arresto de seis a doce fines de semana o multa de tres a seis meses…".* Si la víctima fuera un menor de edad, el delito conllevaría un agravamiento que queda regulado en el **Artículo 184.3** "…*Cuando la víctima sea especialmente vulnerable, por razón de su edad, enfermedad o situación, la pena será de arresto de doce a veinticuatro fines de semana o multa de seis a doce meses en los supuestos previstos en el apartado 1, y de prisión de seis meses a un año en los supuestos previstos en el apartado 2 del presente artículo*…".

Este tipo de situaciones que se produce en las redes sociales y en el que el usuario ve mermada su privacidad, es necesario tomar conciencia de los riesgos que entraña el añadir contactos desconocidos sobre todo en casos de menores de edad, donde la protección que sufren sus datos pueden quedar aireada sino no se tiene un conocimiento mínimo sobre las medidas de privacidad que nos ofrecen estas plataformas.

Los riesgos a menores de edad, están provocando un debate social de gran envergadura del que muchos organismos privados y públicos están tomando buena nota, intentando

llevar a cabo iniciativas junto con los administradores de las redes sociales para que se pueda proteger la intimidad y privacidad de este tipo de usuarios , como :

- Crear herramientas que comprueben la identidad del menor.
- Crear algoritmos de seguridad para detectar acosadores y comportamientos irregulares en las redes sociales, Facebook ya lo está utilizando.

Para concluir este punto, es necesario mencionar que los usuarios adultos de medios sociales deben ser cuidadosos con la publicación en sus perfiles de imágenes de menores de edad, ya lo mencionamos en el punto de datos privados publicados voluntariamente que provocan riesgos a terceros ya que puede ser penado por el **Artículo 4** de **Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil**, ya que podría *"implicar una intromisión ilegítima en su intimidad"* ya que la red social se considera un medio público y las medidas de privacidad pueden ser vulneradas a pesar de restricciones que llevemos a cabo en el sitio web.

3. Ciberbulling

Según indica Antonio Canalda, Defensor del Menor de la Comunidad de Madrid "*el **Ciberacoso o ciberbulling** es un fenómeno que preocupa por la relativa novedad que supone en el comportamiento de nuestros adolescentes, con las consiguientes dudas que pueden generar su abordaje y tratamiento. Entendemos por ciberacoso el acoso de una persona a otra por medio de tecnologías interactivas.".*

En base al informe **"*Ciberbullying: Guía de recursos para centros educativos en casos de ciberacosos*"** publicado en el 2011 por el Defensor de Menor de la Comunidad de Madrid se refleja que de los menores entre 10 y 16 años , un 5,9% de los chicos afirma haber sido víctima de *ciberacoso*, mientras que un 2,9% afirma haber actuado como acosador. De manera que se puede observar el creciente riesgo que entrañan las nuevas tecnologías a la hora de mostrar cualquier forma de acoso o maltrato entre menores de edad; es decir lo que hasta ahora se venía produciendo de forma física toma más fuerza si cabe con los medios sociales donde la agresiones son semejantes a las del contacto físico, se producen amenazas verbales por un grupo o un individuo de forma reiterada contra una víctima que no puede defenderse a través de las redes sociales y

donde se persigue la intimidación de la víctima, en el que se ve inmerso el abuso de poder que ejerce un individuo contra otro, sobre todo en menores de edad donde no existe un control por parte ni de adultos ni de las propias redes sociales.

En el ámbito de las redes sociales, existen varios mecanismos para el acoso como: enviar mensajes amenazadores de forma constante, o mediante la herramienta de chat. Sin embargo, el mayor daño se produce cuando el agresor emplea canales como el perfil del usuario donde el poder de expansión del mensaje es mayor que físicamente, y donde también se pueden colgar imágenes o videos que perjudiquen la intimidad o privacidad para el menor, además de los insultos y comentarios ofensivos que traspasan los límites temporales y físicos que marcaban el acoso en su propio entorno. Otra de las ventajas que ofrecen los medios sociales a este tipo de amenazas o riesgos es el **anonimato,** los acosadores se crean normalmente perfiles con datos personales falsos donde cualquier individuo puede publicar contenidos agresivos o amenazantes contra el menor ya que la protección del acosado es escasa en comparación con el entorno físico ya que nadie puede ayudar al menor y este puede sentirse indefenso frente al acosador. Además la mayoría de estos perfiles son eliminados y es muy difícil posteriormente localizarlos aunque el acosado puede denunciar vía legal este tipo de delitos ya que el contenido queda almacenado en las bases de datos de las propias redes sociales.

2.5.1 Otras amenazas a la privacidad

También podemos hacer referencia a otros tipos de amenazas en las redes sociales y que afectan a aspectos de la vida de un individuo y a la privacidad de estos y de terceros. Atendiendo a la clasificación de (Areito, 2010) se pueden identificar las siguientes:

1. **Expediente-dossier digital de la Información Personal**

   Con la llegada de la minería de datos y la reducción de costo de almacenamiento en disco, posibles terceras partes pueden crear un expediente digital de datos personales con la información revelada de los perfiles de las Redes Sociales. Una vulnerabilidad común es que la mayor parte de los atributos privados que son directamente accesibles por navegación en el perfil también se puede acceder

búsqueda (por ejemplo, el nombre de persona e imagen del perfil es accesible vía navegación en Facebook, MySpace, etc. a menos que la configuración de privacidad por defecto se cambie).Como consecuencia surgen riesgos, así la información revelada en Redes Sociales puede ser explotada por un adversario para avergonzar, chantajear o incluso para dañar la imagen del titular del perfil. Por ejemplo, cada vez más personas ven mermadas sus oportunidades de empleo debido a que el departamento de empleo revisa los perfiles de Redes Sociales de los candidatos posibles. En algunos casos incluso las personas se ven amenazadas, es el caso por ejemplo de Miss New Jersey 2007 que fue amenazada con publicar las imágenes tomadas de su perfil de Red Social Facebook si no entregaba su corona.

2. Reconocimiento Facial

En anteriores apartados, hicimos mención a que muchos de los usuarios de las redes sociales publican imágenes en sus perfiles que pueden ser utilizados para identificar a los titulares de un perfil. De este modo, cualquier atacante puede utilizar estos datos para relacionar perfiles a través de medios que utilizan el reconocimiento facial como parte de una amenaza más amplia.

El reconocimiento facial se puede llevar a cabo mediante el etiquetado de imágenes, además el contenido con el que se acompaña puede ser localizado a través de servicios y sitios Web que nos permiten conectar con el perfil del individuo que estemos buscando; de esta manera el atacante puede recoger datos personales o sensibles produciéndose una intromisión en la privacidad del usuario en cuestión bajo el desconocimiento de éste y sin su consentimiento expreso.

3. Recuperación de imagen basada en Contenido.

Una de las mayores amenazas en la mayor parte de las redes sociales es que aún no tienen instaurados controles de privacidad sobre las imágenes de los perfiles que prevengan revelación de información a través de CBIR (Content Based Image Retrieval). "*CBIR es una tecnología emergente que permite combinar características como aspectos que identifican una habitación (por ejemplo un cuadro) en bases de datos muy grandes y de este modo incrementar las posibilidades de localizar usuarios".* Este tipo de acciones implican una serie de riesgos que pueden desembocar en lo que se conoce como stalking (Amenaza social consistente en acechar a personas). Son

muchos los usuarios que revelan información personal incluyendo localización geográfica, direcciones, lugar de trabajo, lugares de ocio, números de teléfono, etc. en su perfil y que puede ser utilizado por un adversario para llevar a cabo stalking, es decir amenazar a la víctima a través de proximidad física o llamadas telefónicas, correos electrónicos, mensajería instantánea o mensajes en RRSS. El stalking que se lleva a cabo en las redes sociales está aumentando de forma significativa ya que su impacto en un individuo puede variar desde la intimidación y pérdida de privacidad al daño físico y psicológico, marketing no deseado, chantajes y otro tipo de amenazas asociadas con la revelación no deseada de datos de localización.

4. Etiquetado de Imágenes y Cruce de Perfiles

Se presenta una vulnerabilidad consistente en que el usuario de una Red Social tiene la opción de etiquetar las imágenes con metadatos tales como el nombre de la persona de la foto, un link a su perfil de Red Social (incluso si ellos no son los propietarios/controladores de ese perfil) o incluso su dirección de correo electrónico o su teléfono.

Como consecuencia surgen riesgos, así un adversario puede utilizar esta característica para calumniar a ciertas personalidades bien conocidas o para etiquetar y sacar provecho de su reputación.

5. Expediente-Dificultad a la hora de completar el Borrado de una Cuenta Completa

Los usuarios de las redes sociales también se enfrentan a otra amenaza sobre todo a la hora de borrar todos los contenidos de sus cuentas de usuario en cualquier red social. Mucha de esa información secundaria es imposible eliminarla, es el caso de los comentarios públicos que un usuario hace en otras cuentas en las que aparece nuestra identidad y que permanecerán en línea incluso aunque hayamos cancelado la cuenta. A partir de ahí, los usuarios debemos ser consecuentes con el tipo de informaciones que vertemos porque podemos perder el control sobre nuestra propia información personal.

El usuario debe de ser conocedor de que cuando cancelamos una cuenta no todo el contenido se elimina, eso es un falso concepto que los usuarios tienen de los mecanismos de seguridad de las redes sociales ya que la información (datos personales,

direcciones, correo electrónico, teléfonos, mensajes privados, imágenes, etc) eliminada de la cuenta de nuestro perfil queda almacenada .

6. Expediente Ocupación de Perfil por medio de Robo de Identidad

Consistente en que un atacante se puede crear el perfil falso de una persona con los detalles personales de un usuario y crear un perfil suplantando su identidad causándole situaciones incomodas a la persona suplantada. La suplantación de identidad en las redes sociales puede tener consecuencias graves en la victima causando un daño significativo que provoca la intromisión en la privacidad de un individuo y que puede desembocar en la pérdida de su reputación.

7. Spamming

El creciente aumento de medios sociales ha cambiado el concepto de red social como un medio de comunicación entre el entorno más cercano, su expansión también afecta a la publicidad, convirtiéndose en una fuente de difusión para los spammers (productores de correo basura) creando mensajes no deseados llamados spam de red que sobrecargan los perfiles de usuario y pueden causar molestias, pérdida de confianza, así como provocar delitos de phishing-malware o sobrecarga de tráfico, etc.

8. Agregadores de Red Social

Se presenta una vulnerabilidad consistente en que algunas de las nuevas aplicaciones como Snag y ProfileLinker que proporcionan acceso de lectura/escritura a varias cuentas de RRSS para integrar los datos en una única aplicación Web. Pero tales aplicaciones utilizan métodos de autenticación débil de modo que la vulnerabilidad aumenta.

Como consecuencia surgen riesgos, así los efectos de esta vulnerabilidad son robo de identidad, hacer zombis cuentas de RRSS por ejemplo para ataques XSS o publicidad, pérdida de privacidad para otros miembros de la Red Social permitiendo búsquedas a través de una base de datos más amplia.

9. Expediente XSS (Cross Site Scripting), Malware (virus,gusanos,etc).

También "*las redes sociales son vulnerables a ataques* ***Cross Site Scripting*** *y amenazas debidas a widgets producidas por terceras partes.*
Como consecuencia surgen riesgos, así un adversario puede emplear esta vulnerabilidad para comprometer la cuenta, realizar ataques de phishing y difundir contenido no solicitado al correo electrónico y tráfico de IM (Instant Messaging, como Messanger). Además puede utilizarse para ataques de denegación de servicios y la asociada pérdida de reputación" (Areito, 2010).

10. Fuga de Información

La privacidad de las redes sociales está en peligro ya que un atacante puede conseguir ser amigo de un miembro de cualquier grupo privado de usuarios suplantando su identidad para luego acceder a la información privada que pertenece a los miembros de ese grupo exclusivo. De manera, que si las políticas de privacidad no están bien establecidas la información que en ellas se contiene puede sufrir riesgos de fuga si los administradores de redes sociales no emplean mecanismos que eviten el phishing/pharming para información o el spamming, incluso hay alguna como My space que utilizan scripts para invitar amigos.

11. Suplantar Identidad

Las redes sociales son un medio muy propicio para cometer delitos, desde la obtención de información privada de individuos hasta realizar chantajes emocionales u económicos a través de la su suplantación de identidad. Cuando una persona suplanta la identidad de otro perjudica la imagen y el prestigio de un tercero; es recurrente en las redes sociales las suplantaciones de personas públicas (políticos, cantantes, presentadores de televisión, etc.); estos usuarios que toman una identidad que no corresponde con la suya pueden publicar información comprometida, dañando así gravemente la reputación de dichas personas.

Por otro lado tenemos a los hackers, que emplean técnicas más sofisticadas con el fin de obtener las contraseñas de diferentes usuarios a través de técnicas como el phising donde el delincuente implementa un sitio web idéntico a la página de inicio de la red social blanco del ataque y luego realiza envíos masivos no deseados (spam) de un

vínculo a dicha página fraudulenta por correo o mensajes instantáneos, supuestamente con el nombre de la misma red social. Por esta razón los usuarios de las redes sociales deben asegurarse bien de que utilizan claves lo suficientemente seguras y difíciles de descifrar ya que los hackers poseen listas con las contraseñas más comunes, e incluso mucha de la información que utilizamos en nuestros perfiles puede servirles para averiguar la contraseña de los perfiles (nombres familiares, lugares, animales domésticos, seudónimos ,etc); una vez que han accedido a la cuenta el atacante puede entonces apropiarse de varias formas de esta información privada , se adueña del perfil y de los datos que contiene, utilizar el perfil de manera que suplantaría nuestra identidad y atacar a nuestros contactos , reunir más información del usuario atacado desde su perfil o enviar más mensajes spam a través de la plataforma de la red social desde la cuenta secuestrada. Una vez que el delincuente logra robar información de una cuenta, normalmente suele proceder a enviar vínculos que instalen un ladrón de contraseñas en los equipos de sus contactos, lo que se convierte en una propagación.

La apropiación de una cuenta en la redes sociales supone que no solo el riesgo sea hacia la persona en cuestión sino hacía todos los contactos que tiene agregado ese individuo lo que abre el camino a otros delitos como el chantaje o la estafa.

12. Creación de un Perfil Falso

Muchos delincuentes informáticos crean perfiles falsos de forma fraudulenta buscando la confianza necesaria entre los usuarios para ser agregados así sucesivamente hasta establecer vínculos hasta con contactos de amigos.

La creación de un usuario falso comporta la aportación de datos personales ficticios que simulan ser un individuo con el que ganar la confianza de sus víctimas con el objetivo de llevar a cabo actividades delictivas, también existe otro tipo de usuarios que crean perfiles falsos con un fin aparentemente legítimo, ya mencionamos en el apartado de riesgos a la privacidad en menores edad , los daños que podían sufrir como consecuencia del uso de redes sociales; es por eso que muchos padres crean un perfil falso en la red para controlar a sus hijos aunque pueda resultar controvertido llevar a cabo este tipo de acciones porque se puede vulnerar el derecho a la intimidad de un hijo siempre y cuando sea menor de edad.

Por último, algunos usuarios optan por incluir datos falsos en su perfil con el fin de conservar su privacidad (cambios de fecha de nacimiento, nombres, apellidos, ciudad,

etc.) aunque como veremos más adelante es una acción prohibida en las condiciones de uso pero una práctica muy extendida entre los usuarios de los medios sociales, el crear un pseudónimo o el utilizar las iniciales en lugar del nombre real, fecha de cumpleaños falsa, año de nacimiento, etc. La utilización de este tipo de prácticas por un lado tiene sus beneficios (garantizar la privacidad de los datos personales de un individuo) pero por otro se nos presentan una serie de contraindicaciones como que no seamos localizados por nuestros amigos o seamos víctimas de hackers por el tipo de perfil que presentamos estemos expuestos a riesgos.

13. Fraudes en Plataformas Sociales

La suplantación de identidad y la creación de perfiles falsos en las redes sociales, son delitos donde los delincuentes buscan cometer fraudes. Cada vez es más frecuente sobre todo en perfiles de empresas, muchos hackers utilizan un perfil falso para conseguir la confianza del otro, e incluso perfiles personales donde algunos contactos transfieren cantidades de dinero a cuentas, que pueden ser objeto de un delito, o prestamos de cantidades a contactos, que luego resulta que es falso ya que el perfil había sido suplantado por un hacker, etc.

14. Engaños Informáticos

Como anteriormente mencionábamos en el punto de suplantación de identidad en el que los mensajes enviados mediante esta técnica contienen un componente de ingeniería social en el que se intenta engañar a la víctima (destinatario del mensaje) para que visite un determinado sitio web o para que descargue un programa en su ordenador. Un ejemplo claro es Twitter, que emplea el acortamiento de las URL y eso supone que los usuarios estén expuestos a un peligro en el que se puede enmascarar el hecho de que haya enlaces a páginas peligrosas o de origen fraudulento que puede generar daños o sabotajes informáticos.

2.6 Sanciones en las redes sociales

Las redes sociales son plataformas sociales que integran a un numeroso grupo de personas donde se llevan a cabo tanto delitos contra los derechos de los individuos como a los que afectan a la tecnología.

Las personas que llevan a cabo este tipo de ataques o delitos en redes sociales no son ajenos al descuido que los usuarios hacen de la información personal que vuelcan en las redes sociales; los usuarios pierden el sentido de protección de la información personal que publican y no son conscientes de los mecanismos de privacidad que publican en las políticas de privacidad de estas plataformas. Algo que llama poderosamente la atención cuando de forma física los individuos no revelamos aspectos de nuestra intimidad y privacidad pero a través de nuestros perfiles en las redes sociales brindamos acceso a una gran cantidad de información sensible al alcance de cualquier hacker o delincuente.

De nada sirve mantener la privacidad en el entorno físico si luego publicamos en una red social mediante entradas en el muro, actualizaciones de estado o fotos de nuestras momentos más privados donde los desconocidos pueden obtener información relevante que damos a conocer donde mostramos todos los datos personales, como: ubicación geográfica, nombre completo, teléfonos, lugar de trabajo, nivel económico (a través de una imagen de nuestra casa, o de un coche) los delincuentes pueden conocer aspectos muy íntimos de nuestra vida ayudados por los sistemas de localización que ofrecen información en tiempo real de la ubicación de los individuos.

En apartados anteriores, definimos cuáles son los derechos que son vulnerables para perpetrar delitos y ahora mostramos cuáles son los delitos que se pueden llevar a cabo contra ese tipo de derechos en las redes sociales y cuáles son las sanciones amparadas por la legislación.

1. Sanciones contra el Derecho al Honor

Las redes son un blanco fácil para llevar a cabo delitos contra el honor donde un individuo puede ver afectado su derecho a través de una calumnia u ofensa; la legislación española sanciona la calumnia con sanciones de 4 a 10 meses. Si la ofensa o calumnia se hace a través de medios publicitarios entre ellos las redes sociales la pena será de **prisión** de 6 meses a 2 años, o una sanción de 6 a 24 meses. A parte de los usuarios que cometen este tipo de delitos también las personas físicas o jurídicas son responsables de que el delito se difunda por los medios de comunicación aunque ellos suelen alegar en sus políticas de privacidad que se eximen de cualquier responsabilidad del contenido que sea publicado por los usuarios.

Además si la persona que injuria se ve condicionada a cometer un delito por una comisión económica o recompensa podrá ser además inhabilitado para el ejercicio de su cargo público, oficio o profesión por un tiempo comprendido entre 6 meses y 2 años cuando esas calumnias se dirijan contra cargos públicos que estén en ese momento en ejercicio sobre faltas penales o infracciones administrativas, el responsable puede quedar exento de su responsabilidad si se puede demostrar que las manifestaciones, comentarios que se vierten son ciertos. También los responsables pueden quedar exentos de culpabilidad si el ofendido o su representante legal, que actúa en su nombre deciden dejar libre de toda responsabilidad al delincuente todo ello antes de que la sentencia de una autoridad judicial sea firme.

En relación a las consecuencias penales anteriormente mencionadas, el responsable de los delitos de injuria o calumnia está obligado a subsanar el daño ocasionado mediante una **remuneración económica** a favor de la persona calumniada, es lo que se denomina **responsabilidad civil**; esa responsabilidad también la asume la persona física o jurídica que administra el medio de comunicación donde se haya propagado la calumnia o injuria. En el caso de la red social dada la novedad del medio; la legislación no atribuye de forma específica la responsabilidad de un delincuente que atente contra el honor de un individuo.

2. Sanciones contra la Libertad

La legislación española sanciona con cárcel a todos aquellos individuos que comentan un delito de amenazas con una sanción de 1 a 5 años, si el daño se ve condicionado por un agravante como por ejemplo un chantaje u extorsión, las penas serán de 2 a 6 años de prisión. Hay que tener en cuenta que la comisión de este tipo de delitos son penados en función de cómo se hayan llevado a cabo, se agrava el delito si las amenazas o coacciones se realizan por medios de comunicación (teléfonos, internet, televisión u otros), mientras también hay delitos que no son constitutivos de cárcel pero si de multas con prisión de 2 meses a 2 años o multa de 12 a 24 meses. Si es un delito de coacción la pena de cárcel es de 6 meses a 3 años o una multa de 6 a 24 meses, todo ello depende de la gravedad de la coacción o de los medios que se empleen en la comisión del delito.

3. Sanciones contra la Propiedad Intelectual e Industrial

Según la legislación española cuando se distribuye o publica de forma pública contenido protegido por derechos de autor y no existe ánimo de lucro, este tipo de comportamiento no suele ser penado en España.

En cuanto a las sanciones que tienen que ver con la propiedad intelectual e industrial, queda señalada en el **Código Penal** en los **Artículos 270 a 276**. En el **Artículo 270** se establece penas de cárcel de los 6 meses a los 2 años y sanciones de 12 a 24 meses a aquellos que con ánimo de lucrarse y causen daños a un tercero, reproduzcan, plagien, distribuyan o comuniquen públicamente una obra sin la autorización de los titulares de los derechos de propiedad intelectual, en el caso del **Artículo 272** se hace una remisión remite a las indemnizaciones que quedan establecidas en el **Real Decreto Legislativo1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual** a los **Artículos 138 a 140**.

El **artículo 138 de la LPI** se dicta "*que el titular de los derechos reconocidos en esta ley, sin perjuicio de otras acciones que le correspondan, podrá instar el cese de la actividad ilícita del infractor y exigir la indemnización de los daños materiales y morales causados"*. La indemnización relacionada con los daños y perjuicios en la que el responsable de incumplir dicho derecho deberá comprender por un lado el valor de la pérdida que haya sufrido además de la ganancia que haya dejado de obtener a causa de la violación de su derecho. Y el infractor debe de abonar una cuantía indemnizatoria que incluye los gastos de investigación en los que se haya incurrido para obtener pruebas razonables de la comisión de la infracción objeto del procedimiento judicial.

En los **Artículos 273 y 274** también se especifica las penas con cárcel de 6 meses a 2 años y las sanciones de 12 a 24 meses para aquellos que "*utilicen, con fines industriales o comerciales, sin consentimiento del titular, con conocimiento de su registro, objetos amparados por derechos de Propiedad Industrial"* o "*quien reproduzca un signo distintivo de un producto protegido"* (**Artículo 274**). En cuanto a la aplicación de este tipo de legislación en redes sociales comentamos en el primer párrafo de este epígrafe que en estas plataformas presumiblemente no hay un ánimo de lucro como para cometer delitos contra la propiedad industrial e intelectual pero se pueden presentar algunos contratiempos como por ejemplo, y eso sí que puede ocurrir es que una marca busque perjudicar a otra marca de su competencia con tal de obtener un beneficio económico.

4. Sanciones contra la Protección de Datos

Atendiendo a la **Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal** (LOPD) vigente en la legislación española las sanciones que se imponen toman una graduación en función de la gravedad de dichos delitos:

- Las infracciones leves, engloban desde la no rectificación o cancelación de las solicitudes de datos con sanciones entre 601,01€ y 60.101,21€.
- Las infracciones graves, incluye motivo de delito el tratar datos protegidos sin la autorización de un tercero, lo que conlleva sanciones entre 60.101,21€ y 300.506,25€.
- Y por último, las infracciones muy graves, como la recogida de datos de manera engañosa o fraudulenta, con sanciones entre 300.506,25€ y 601.012,1€.

3. Marco jurídico

En este capítulo vamos a abordar los aspectos jurídicos vistos en el proyecto, analizando todas aquellas leyes que tengan una relación con la garantía de la privacidad en las redes sociales.

Las redes sociales se han convertido en herramientas de comunicación con una gran relevancia social que favorecen la relación entre personas y con ello la transmisión de información entre distintos individuos en diferentes entornos. Desde que un usuario decide registrase en una red social está suscribiendo un contrato en el que debe de incluir una serie de datos e informaciones personales; crearse un perfil en una red social es un acuerdo entre un servicio que tiene un carácter gratuito y un individuo donde el usuario cede su privacidad. Es por esta razón que las redes sociales deben de asumir el compromiso de salvaguardar y proteger una serie de derechos relacionados con la privacidad del usuario, es necesario determinar los aspectos más relevantes y cuáles son los que están sometidos en la legislación vigente. Conocer el elemento jurídico en las redes sociales es uno de los aspectos más fundamentales no solo para los usuarios sino también para los juristas a la hora de elaborar las futuras normas jurídicas. Los aspectos más importantes que se deben de analizar para realizar un análisis legislativo en las redes sociales son: la protección de datos de carácter personal, protección de la

privacidad, honor, intimidad, imagen así como el derecho de propiedad intelectual e industrial; incluyendo en cada uno de estos derechos la regulación específica y especial que poseen.

3.1 Legislación Española

El marco jurídico al que se ha venido haciendo alusión a lo largo de la exposición realizada en este proyecto se corresponde con la siguiente legislación:

- **Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y familiar y a la propia imagen.**

- **Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.**

- **Directiva europea 95/46 CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995 relativa a la Protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación.**

- **Ley 10/1989, de 14 de diciembre, de Protección de Menores.**

- **Ley 1/1995, de 27 de enero, de Protección del Menor.**

- **Ley orgánica 10/1995, de 23 de noviembre, del Código Penal.**

- **Ley orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.**

- **Real decreto legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.**

- **Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).**

- **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la información y de Comercio Electrónico (LSSI-CE).**

- **Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.**

- **Real decreto 1720/2007 de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la ley orgánica 15/1999, de protección de datos de carácter personal (RLOPD).**

A continuación se llevará a cabo una descripción más profunda sobre los artículos y referencias de la legislación vigente española que pueden aplicarse a las redes sociales, en relación a los distintos derechos analizados a lo largo del proyecto y que están relacionados con la privacidad.

1. Protección de Datos de Carácter Personal

Uno de los principales aspectos que podemos analizar jurídicamente sobre las redes sociales en la normativa española, es el relacionado con la protección de datos de carácter personal, regulada en la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)** y su reglamento de desarrollo, **Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RLOPD) y la Ley 34/2002,de 11 de Julio , de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE)** .

La Ley Orgánica 15/1999 sobre la Protección de Datos de Carácter Personal (LOPD) fue aprobada el 14 de Diciembre de 1999, en esta norma jurídica se establecen una serie de obligaciones para los titulares de datos personales de empresas y administraciones públicas.

En lo que respecta a las redes sociales podemos hacer mención a varios artículos dentro de esta Ley, destacando entre ellos:

El **Artículo 2,** se hace referencia al ámbito de aplicación, en el caso de una red social con sede en otro país, los datos recogidos mediante ordenadores españoles, se regirán por la LOPD también.

Artículo 2. Ámbito de aplicación.

1. ***La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.***

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:
a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:
a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:
a) Los ficheros regulados por la legislación de régimen electoral.
b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

En el Artículo 3, se definen algunos conceptos relacionados con la protección de datos, entre ellos: *Datos de carácter personal, Fichero, Tratamiento de datos, Responsable del fichero o tratamiento, Afectado o interesado,* ***Procedimiento de disociación***, ***Encargado del tratamiento***, ***Consentimiento del interesado***, ***Cesión o comunicación de datos***, ***fuentes accesibles al público***.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), es una de las normativas más importantes donde se definen los derechos que tienen los usuarios en Internet, y consecuentemente a los usuarios de las redes sociales. Donde aparte de garantizar los derechos de los ciudadanos en materia de protección de datos, incluye algunas **obligaciones** para los responsables de ficheros de tratamiento de datos de carácter personal.

En el **Artículo 4** se manifiesta que los responsables del fichero también tendrán que velar por la **calidad de los datos,** unos datos que deben "*ser adecuados, pertinentes o no excesivos en relación con el ámbito y finalidades legítimas para las que se han obtenido, no podrán usarse para finalidades distintas de aquellas para las que fueron recogidos. Deberán ser exactos y actualizados.*

Si son inexactos o están incompletos deben ser cancelados o sustituidos por los correctos. Serán cancelados cuando dejen de ser necesarios. No podrán ser conservados una vez que dejen de ser útiles para la función prevista, con excepción de la legislación específica prevista al efecto". En el **Artículo 5,** se proporciona toda aquella información necesaria para los interesados que se soliciten datos personales.

Artículo 5. Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

El **Artículo 6** expone que el tratamiento de los datos de carácter personal requiere el consentimiento del afectado; en el **Artículo 13** los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativo por lo que pueden impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento. Y por último, el **Artículo 19** donde se presenta el derecho de consulta, acceso, rectificación y cancelación donde los ciudadanos pueden ser indemnizados en caso de sufrir daño o lesión en sus bienes o derechos.

También debemos de destacar algunos artículos importantes en esta ley**,** como el **Artículo 7** donde se hacen referencia a los datos especialmente protegidos como la ideología, religión, y creencias. En **el Artículo 8** versa sobre los datos relativos a la salud; en ambos es de carácter obligatorio avisar al interesado sobre su derecho a no prestar su consentimiento sobre datos especialmente sensibles relacionados con el origen racial, salud o vida sexual salvo que lo regule una ley.

Artículo 7. Datos especialmente protegidos.

1. *De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.*

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos

relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Mientras el **Artículo 9**, señala que el responsable del tratamiento de datos es quien debe ejercer de responsable que garantice la seguridad de los datos de carácter personal y para ello debe de llevar a cabo una serie de medidas. Ningún fichero debe registrar datos de carácter personal que no reúnan las condiciones que se rija en la normativa basada en la integridad y seguridad ,así como a la referente a la de los lugares de tratamiento, locales, equipos, sistemas y programas que lo forman.

Artículo 9. Seguridad de los datos.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

El **Artículo 10**, señala que el profesional está obligado al **deber de secreto,** incluso después de haber finalizado su vinculación profesional o personal con el titular o el responsable del fichero. Los **Artículos 12 y 13** son los más importantes ya que es donde la ley señala la **comunicación de datos a terceros**, donde un individuo debe ser el que ceda mediante consentimiento los datos al cedente, con la suficiente información para saber o conocer cuál la finalidad a la que irán destinados los datos que se han transmitido y que se han autorizado para una determinada actividad. En cuanto a la creación de ficheros de datos de carácter personal, el **Artículo 26** señala que toda persona o entidad debe de comunicar los detalles del fichero y notificarlo con anterioridad a la Agencia de Protección de Datos; mientras el **Artículo 27** enuncia que cuando las personas finalizan su prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento al igual que si el responsable del fichero quiera efectuar una cesión de datos, deberá informar de ello a los afectados, indicando la finalidad del fichero, la naturaleza de los datos y el nombre y dirección del cesionario.

El **Artículo 30**, señala los tratamientos de datos con fines de publicidad y de prospección comercial, donde el responsable del fichero debe comunicar al interesado el origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le amparan. Según el **Artículo 33,** se estipula que no pueden realizarse transferencias de datos de carácter personal a países que no proporcionen un **nivel de protección equiparable** al que se regula en España, salvo que se obtenga autorización previa del Director de la Agencia de Protección de Datos atendiendo a unas garantías adecuadas para el tratamientos de los datos aunque hay algunas excepciones como cuando se transfieren datos de carácter personal a nivel internacional para convenios o tratados en los que España forma parte.

Y por último, destacan los **Artículos 43 a 49** donde los responsables de los tratamientos de datos y de los ficheros estarán sujetos al **régimen sancionador** que se establece en esta ley, donde se obliga a estos a pagar una serie de sanciones a la Agencia de Protección de Datos por las infracciones acaecidas. Dicha ley establece una clasificación para este tipo de comportamientos y que a continuación mostramos el **Artículo 44** donde se estipulan.

Artículo 44. Tipos de infracciones.

1. ***Las infracciones se calificarán como leves, graves o muy graves***.

2. Son infracciones leves*: a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda. b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos. c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave. d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley. e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.*

*3. **Son infracciones graves:** a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente. b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad. c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible. d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.*

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada. f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara. g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo. h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen. i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos. j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos. l) Incumplir el deber de información que se establece en los Artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

***4. Son infracciones muy graves**: a) La recogida de datos en forma engañosa y fraudulenta. b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas. c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del Artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del Artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del Artículo 7.*

También en el **artículo 55** se expone que en determinadas situaciones en las que el **artículo 18** dejará de aplicarse en caso de *"puedan ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución"* .A raíz de estos principios fundamentales se crea una de la leyes más importante en cuanto a los datos de carácter personal y los medios tecnológicos , aprobándose en 1992 **Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal** (**LORTAD**) aunque solo tenía aplicación para los ficheros de carácter personal que se tratan en soportes automatizados, hoy en día se encuentra derogada. La LOPD amplía el ámbito de aplicación a todo tipo de ficheros de carácter personal, sin importar el tipo de soporte en el cual se traten donde se tiene como objetivo garantizar y proteger, todo lo que respecta al tratamiento de los datos personales, las libertades y los derechos fundamentales de las personas físicas, sobre todo los relacionados con el honor e intimidad personal y familiar.
A nivel europeo, se aprueba una normativa relacionada con la protección de las personas físicas y el tratamiento de los datos personales, así como la difusión de estos; es la **Directiva Europea 95/46 CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995 relativa a la Protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación** publicada el 24 de Octubre de 1999.

En cuanto a **la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE)** una normativa básica en la regulación de los servicios prestados a través de sitios web o todo sitio web, donde se establecen una serie de requisitos:

- ***Que el prestador de servicios de la sociedad de la información*** -responsable del sitio web- ***se encuentre establecido en España***, es decir, cuyo domicilio social se encuentren en cualquier parte del territorio español y sea el lugar donde se lleven a cabo la gestión del negocio y las tareas administrativas.

- Que el prestador, ***a pesar de encontrarse en otro Estado***, ofrezca sus servicios a través de una sede permanente situada en España, donde realice toda o parte de su actividad.

- Que el sitio web, ***a pesar de ser propiedad y alojarse en servidores externos a la Unión Europea***, dirijan sus servicios específicamente al territorio español

Por lo que quedan sujetos a las obligaciones legales de nuestro país salvo que esto no vaya en contraposición de lo establecido en tratados o convenios internacionales.

Los criterios que establece esta ley son para determinar el ámbito de aplicación de los sitios web o todos tipo de servicios aunque la mayoría de las redes sociales que utilizamos en España tiene su sede en Estados Unidos y que no disponen de relación con nuestro país, y eso que este tipo de plataformas cuentan con millones de usuarios de España. Son muchas las redes sociales que ni siquiera operan con el dominio de nuestro país. Así se establece en el **Artículo 2.3** de dicha ley donde expone ***la utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio***, donde establece que no es un requisito indispensable que se cuente con un sede permanente en nuestro país aunque si se disponga de forma habitual de instalaciones o lugares de trabajo, en los que se realice toda o parte de su actividad. Este hecho, complica si cabe aun más la aplicación de las normativas en España a las redes sociales así como las acciones o resoluciones contra dichas plataformas. También el **Artículo 4** de la LSSI, enuncia que los prestadores que dirijan sus servicios específicamente al territorio español quedan sujetos a su ámbito de aplicación.

En el **Artículo 16,** dicha ley establece que este tipo de servicios, al limitarse a almacenar datos facilitados por los usuarios carecerían de una obligación general de previa supervisión sobre los contenidos añadidos por éstos. Además dentro de este artículo también se menciona que si existe conocimiento sobre la ilicitud, se actúe con la diligencia necesaria para retirar dichos datos o imposibilitar el acceso a ellos, para ello debe ser un órgano competente quien haga esta declaración y declare la lesión*" cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución"*

Esta ley tiene un peso importante sobre todo en la promoción empresarial en las redes sociales , como servicios que forman parte de la sociedad de la información; así como

la comunicación comercial que se lleva a cabo con el fin de dirigir a un público una imagen o servicios de una marca ya pueda ser profesional o personal. Esta ley **en el Artículo 21** refleja que no se considera comunicación comercial a aquellos datos directos que tengan que ver con una actividad de un tercero, tanto si es una persona particular como una empresa incluyendo (dirección de correo electrónico, comunicaciones, o servicios que hayan sido elaborados por un tercero y no haya habido compensación económica). Si queremos constituir una comunicación comercial se deben de aplicar los criterios que se formulan en los **Artículos 19 al 22** de dicha ley como por ejemplo: consentimiento expreso de los clientes (opt-in o opt- out), informaciones claras sobre la publicidad si es una promoción, concurso, y ofrecer la posibilidad de revocar el consentimiento o oponerse a dicha comunicación comercial.

Y por último, no se puede obviar el hacer mención en lo que respecta a protección de datos personales a la **Ley 25/2007 de 18 Octubre, de Conservación de datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones,** donde en los **Artículos 1 y 6** se refleja que "los *datos de tráfico sólo pueden ser cedidos previa autorización judicial y con fines de detección, investigación y enjuiciamiento de delitos graves "* estas palabras son similares a las que se señalan en el **Artículo 40** de la LOPD .

Artículo 40. Potestad de inspección.

1. *Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.*

A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

2. Protección al Honor, Intimidad e Imagen

Otro de los derechos fundamentales que hemos citado a lo largo del proyecto es el Derecho al Honor, Intimidad e Imagen que toda persona tiene y que está amparada en la principal norma jurídica de nuestra legislación, la Constitución de 1978 donde se hace mención a aspectos relacionados con la intimidad, el honor destacando el artículo 18, es la primera apreciación en nuestra normativa donde se hace mención a dicho derecho en la legislación.

Artículo 18 de la Constitución Española.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Pero la protección de estos derechos se encuentran regulados en la **Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen,** y cuyo fin es proteger a los individuos de todo tipo de intromisiones ilegítimas y no autorizadas expresamente por el titular y que afecten de forma directa a su honor, intimidad propia o familiar, así como a su imagen. En este sentido, cabe señalar la Sentencia **STC 83/2002, de 22 de abril, sobre INTIMIDAD y PROPIA IMAGEN** donde se le otorga al demandante su derecho a la intimidad e imagen frente al recurso de casación presentado por la compañía mercantil Editorial Gráficas Espejo, S.A por la publicación de unas fotografías en la revista Diez Minutos.

En las redes sociales al igual que en la vida física la protección de datos, la intimidad y la protección de la imagen de las personas debe ser esencial ya que en dichas

plataformas se intercambian informaciones personales no solo de un individuo concreto sino que pueden afectar a terceros.

La Ley Orgánica 1/1982 regula desde el punto de vista civil la protección de un derecho y tiene un vínculo estrecho con la LOPD pero abarca una regulación inferior y menos amplia frente a la de protección de datos de carácter personal pero abarca un ámbito jurisprudencial más extenso y desarrollado. Como es el caso de los menores de edad donde por ejemplo en el **Artículo 3.2** de la Ley Orgánica 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen se señala que *"el consentimiento habrá de otorgarse mediante escrito por su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado. Si en el plazo de ocho días el Ministerio Fiscal se opusiere, resolverá el Juez"*.

Las redes sociales son las responsables de proteger la privacidad e intimidad y sus políticas de los usuarios y son los que deben cumplir con un adecuado sistema que englobe tanto el diseño de la plataforma como el control de las herramientas puestas al servicio del usuario y que son las que van a garantizar o evitar los problemas relacionados con la privacidad , lo que se denomina "Privacy by Design" . Los diseñadores de redes sociales como cualquier otro sistema o arquitectura de sistema que se constituye deben de consignar una serie de estándares relacionados con la privacidad aunque no son exclusivos a redes sociales como:

- Privacy Framework (ISO-IEC CD 29100)
- Privacy Reference Architecture (ISO-IEC WD 29101)
- Para certificar la gestión de seguridad (UNE-ISO /IEC 27001:2007)
- Para establecer modelos de madurez (proposal on a Privacy Capability Maturity Model (ISO-IEC NP 29190) incluso un sello de privacidad como (EuroPrise-European Privacy Seal) .

Es por esta razón, que las legislaciones que se van formulando exigen a los administradores de las redes sociales de que no lleven a cabo actos que vulneren la intimidad de los mismos.

3. Protección a la Propiedad Intelectual

La Propiedad Intelectual en España está regulada en la **Ley de Propiedad Intelectual de 1/1996, de 12 de abril (modificada por la Ley 23/2006, de 7 de julio)**. Esta ley protege las obras originales y creaciones artísticas, literarias o científicas, a las que por su mera creación, integran una serie de derechos de carácter personal y patrimonial, y que le atribuyen al autor la plena disposición y el derecho exclusivo para explotar dichas obras, sin más límites que los que establece la legislación. El titular de un derecho de propiedad intelectual, es la persona que puede autorizar o no la reproducción total o parcial, así como la disposición o transmisión de una obra, salvo en algunas excepciones mencionadas en la legislación y que son entre otras; el derecho de cita, los trabajos de actualidad o las reproducciones provisionales y copias privadas.

Aunque nos parezca que la propiedad intelectual no tiene relación con las redes sociales no es así, estos sitios web colaborativos centran sus funcionalidades en el intercambio de información. Son el lugar idóneo para publicar y generar contenidos sobre todo de materiales gráficos como fotografías y vídeos, y cuya autoría corresponde en su mayoría a terceros aunque también hay obras cuya propiedad intelectual es del mismo usuario del perfil, es decir, de autoría propia como: publicar obras musicales, videos u obras intelectuales cuyo finalidad es promocionarlas a través de la red para su mayor difusión, este tipo de situaciones está generando enfrentamientos y dilemas jurídicos respecto a la explotación de las obras intelectuales a través de estas plataformas.

Al igual que hicimos en la legislación sobre protección de datos de carácter personal, vamos a enunciar algunos artículos de la ley que provocan conflictos respecto a las redes sociales, entre ellos destacan los derechos morales, a los que un autor no puede renunciar y los derechos de explotación que si pueden ceder. Por ejemplo el **Artículo 14** incluido a continuación versa sobre los derechos morales.

Artículo 14.

Contenido y características del derecho moral

Corresponden al autor los siguientes derechos irrenunciables e inalienables:

1. Decidir si su obra ha de ser divulgada y en qué forma.

2. Determinar si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente.

3. Exigir el reconocimiento de su condición de autor de la obra.

4. Exigir el respeto a la integridad de la obra e impedir cualquier deformación, modificación, alteración o atentado contra ella que suponga perjuicio a sus legítimos intereses o menoscabo a su reputación.

5. Modificar la obra respetando los derechos adquiridos por terceros y las exigencias de protección de bienes de interés cultural.

6. Retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y perjuicios a los titulares de derechos de explotación. Si, posteriormente, el autor decide reemprender la explotación de su obra deberá ofrecer preferentemente los correspondientes derechos al anterior titular de los mismos y en condiciones razonablemente similares a las originarias.

7. Acceder al ejemplar único o raro de la obra, cuando se halle en poder de otro, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda. Este derecho no permitirá exigir el desplazamiento de la obra y el acceso a la misma se llevará a efecto en el lugar y forma que ocasionen menos incomodidades al poseedor, al que se indemnizará, en su caso, por los daños y perjuicios que se le irroguen.

En el **Artículo 17** de dicha ley se enuncian los derechos de explotación que si se pueden ceder respecto a los derechos patrimoniales, y señala que "*corresponde al autor el ejercicio exclusivo de los derechos de explotación de su obra en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser realizadas sin su autorización, salvo en los casos previstos en la presente Ley*". Estos derechos patrimoniales tienen una vigencia durante toda la vida hasta después de su muerte, si el autor es una persona física si es una persona jurídica, la vigencia de los derechos patrimoniales es desde los 50 años siguientes a su divulgación o, en caso de que no haya sido sometida a dicha acción de

divulgación se tomará la de creación. En los **Artículos 18 al 21** de la presente ley se incluyen dichos derechos patrimoniales, entre los que se incluyen:

- **Derecho de reproducción**

La reproducción es la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda una obra o de parte de ella, que permita la transmisión, comunicación o la obtención de copias.

- **Derecho de distribución**

Es la disposición para el público del original de una obra, así como de las copias en un soporte tangible, mediante su venta, alquiler, préstamo o de cualquier otra forma.

- **Derecho de comunicación pública**

Es todo acto por el cual un conjunto de personas pueda tener acceso a una obra sin previa distribución de forma individual. No se considera comunicación pública, todo aquello que se lleve a cabo en un ambiente intimo o privado de carácter domestico salvo si está integrado o conectado a una red que tenga una difusión de cualquier tipo.

- **Derecho de transformación**

Comprende la traducción, adaptación y cualquier otra modificación en la forma esencial de la obra y que derive en otra completamente distinta. La obra modificada, traducida o adaptada, así como sus derechos de propiedad intelectual corresponderán al autor de la modificación sin ello conllevar perjuicios al autor de la obra original que seguirá conservando los derechos de la obra existente de autorizar, durante todo el plazo de protección los derechos sobre ésta, incluyendo la explotación en cualquier forma y con ello su reproducción, distribución, comunicación pública o nueva transformación.

También es importante señalar, una de las modificaciones más importante que tiene la ley 23/2006 de Propiedad Intelectual sobre los cambios establecidos sobre una compensación equitativa por copia privada a los autores, artistas, editores y productores por obras divulgadas en publicaciones, fonogramas, videogramas u otros soportes sonoros, visuales o audiovisuales. Respecto a las redes sociales, los usuarios compartimos obras, documentos sonoros o audiovisuales de los que no somos autores por lo que nos debemos de asegurar que dicho acto de explotación este debidamente autorizado por los titulares de la obra o este permitido por la ley, como se enuncia en el **Artículo 31.2** *"donde se respeten las condiciones de acceso legítimo y uso no colectivo*

ni lucrativo de las obras"; los actos de explotación posteriores que de un usuario a una obra dependerá de las condiciones de uso o licencia(no todas las obras que aparecen en Internet son consistentes de publicarlas en una red social ni de realizar copias).

Artículo 25.

Compensación equitativa por copia privada

1. La reproducción realizada exclusivamente para uso privado, mediante aparatos o instrumentos técnicos no tipográficos, de obras divulgadas en forma de libros o publicaciones que a estos efectos se asimilen reglamentariamente, así como de fonogramas, videogramas o de otros soportes sonoros, visuales o audiovisuales, originará una compensación equitativa y única por cada una de las tres modalidades de reproducción mencionadas, en favor de las personas que se expresan en el párrafo b) del apartado 4, dirigida a compensar los derechos de propiedad intelectual que se dejaran de percibir por razón de la expresada reproducción. Este derecho será irrenunciable para los autores y los artistas, intérpretes o ejecutantes.

2. Esa compensación se determinará para cada modalidad en función de los equipos, aparatos y soportes materiales idóneos para realizar dicha reproducción, fabricados en territorio español o que hayan sido adquiridos fuera de éste para su distribución comercial o utilización dentro de dicho territorio.

Para proceder a la lícita explotación de contenidos protegidos ajenos a través de las redes sociales es necesario que los usuarios queden amparados por algunos actos que se permiten en la Ley de Propiedad intelectual, que son el régimen de excepciones donde la ley determina que actos no autorizados son lícitos o constitutivos de infracción recogidos en los **Artículos 31 y siguientes**.

De todos ellos los más vinculantes con las redes sociales son:

- El **Artículo 32.1 pfo.1**, dice que "*es lícita la inclusión en una obra propia de fragmentos de otras ajenas(o de obras aisladas de carácter plástico o fotográfico), a titulo de cita o para su análisis comentario o juicio, siempre que se realice con fines docentes o de investigación [….]".*

- **El Artículo 32.2 pfo.2**, *"las recopilaciones periódicas en forma de reseñas o revistas de prensa tendrán la consideración de cita y están permitidas*".
- El **Artículo 33.1**, recoge que *"los trabajos y artículos sobre temas de actualidad difundidos por los medios de comunicación social pueden ser reproducidos, distribuidos y comunicados públicamente por otros medios de comunicación social."*
- El **Artículo 33.2**, enuncia que *"las conferencias, alocuciones e informes pronunciados en público pueden ser reproducidas, distribuidas y comunicadas al público libremente por cualquiera con el fin de informar sobre la actualidad"*.
- El **Artículo 35.1**, enuncia que "*no es necesaria autorización alguna para las obras susceptibles de ser vistas u oídas con ocasión de informaciones sobre acontecimientos de actualidad"*.
- El **Artículo 35.2**, enuncia que *"las obras situadas permanentemente en vías públicas pueden ser reproducidas, distribuidas y comunicadas libremente por cualquiera, por medio de dibujos, fotografías y procedimientos audiovisuales"*.
- El **Artículo 39**, enuncia *"que no exige consentimiento del autor la parodia de la obra divulgada, mientras no implique riesgo de confusión con la misma ni infiera un daño a la obra original o a su autor*".

4. Protección a la Propiedad Industrial

Los derechos de propiedad industrial son privilegios absolutos o de exclusión que solamente se adquieren mediante la inscripción en un registro especial de la propiedad. En España, la Oficina Española de Patentes y Marcas (OEPM) protege las distintas modalidades de propiedad industrial. Hay dos modalidades de propiedad industrial: 1. Los signos distintivos del empresario (autónomo o persona jurídica), el establecimiento y los productos o servicios (el nombre comercial y las marcas), que se protegen porque permiten su distinción respecto a los demás. Las marcas permiten a su titular distinguir su producto de cualquier otro, aunque sea de la misma naturaleza, de modo que alguno productos acaban denominándose con el nombre de la marca (por ejemplo, "Coca-Cola" es la marca de un refresco de cola, y "Kodak" de fotografía).

Por otro lado, las patentes, modelos de utilidad, dibujos industriales y artísticos, (ver glosario) que son susceptibles de protección como creaciones intelectuales porque aportan soluciones a problemas tecnológicos o de diseño y tienen una amplia proyección en el terreno económico.[18] Son susceptibles de protección aquellos inventos que sean **novedosos,** por lo que la patente protege sobre todo una idea que se plasma a través de diseños, modelos o dibujos que se registran para que nadie pueda reivindicar la autoría de los mismos, y por tanto, para poder explotarlos económicamente. Debido a esto, los usuarios no podrán subir contenido que incluya signos distintivos protegidos ni creaciones intelectuales, industriales y artísticas susceptibles de protección.

5. Protección a Menores de Edad

Como mencionábamos en apartados anteriores, los menores de edad son uno de los tipos de usuarios más vulnerables en las redes sociales, que se han convertido en lugares de comunicación y participación donde niños y jóvenes establecen vínculos amistosos con otros, además de suministrar e intercambiar todo tipo de información y contenidos personales: datos de contacto, fotografías, aficiones, vídeos, etc**.** Dichas acciones conllevan una serie de **riesgos para la privacidad y para la propia seguridad del menor e, incluso, de su entorno.** Un entorno que pocas veces es consciente de los peligros que entraña el no tomar medidas de control y defensa de los derechos de nuestros menores, por esta razón la primera responsabilidad la deben de ejercer los padres junto a las medidas jurídicas que se establecen en las normativas vigentes, como en el reciente **Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD***)*, concretamente en el **artículo 13** es donde se dispone una serie de requisitos de naturaleza obligatoria cumplimiento para tratar los datos de los menores:

El Artículo 13.1 del citado reglamento se dispone el consentimiento que los mayores de 14 años deben de dar para tratar sus datos, así como la obligatoriedad de padres o tutores legales tienen que dar para autorizar la obtención de datos *"Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos caso en los que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de menores de catorce años se requerirá el consentimiento de los padres o los tutores".*

En el **Artículo 13.2** del citado RLOPD, **se** establecen una serie de límites en relación a los datos que se pueden obtener del menor y de su entorno sin consentimiento previo y dispone que:

"En ningún caso podrán recabarse del menor ***datos que permitan obtener información sobre los demás miembros del grupo familiar****, o sobre las características del mismo, como los datos relativos a la* ***actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros****, sin el consentimiento de los titulares de tales datos. (...)".*

El Artículo 13.3, enuncia que la información que se facilite a los menores utilice un lenguaje sencillo que pueda ser entendido.

"Cuando el tratamiento se refiera a datos de menores de edad, ***la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible*** *por aquéllos, con expresa indicación de lo dispuesto en este artículo.*

El **Artículo 13.4**, enuncia la verificación de la edad del menor, la ley obliga a toda entidad que recabe o trate datos de menores "*articular los* ***procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor"*** así como, en su caso, *"****la autenticidad del consentimiento prestado (…) por los padres****, tutores o representantes legales."*

En definitiva, y sobre todo en el caso de Internet y redes sociales es una cuestión difícil de controlar; ya que los titulares del servicio no debe fiarse únicamente de la información facilitada por el menor a través de un mero formulario sino que debe establecer algún mecanismo adicional para comprobar su veracidad, deben de establecer sistemas o procedimientos que mejoren los mecanismos para comprobar y verificar la actual edad del menor y la autenticidad del consentimiento de sus progenitores, en su caso.

Por otro lado, existen otra serie de normativas relevantes para proteger los derechos que afectan a los datos de los menores y sus representantes legales. Dichos derechos están reconocidos en la propia **Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)** en el **Artículo 15** se enuncia el derecho de acceso **y en el Artículo 16** el derecho de rectificación y el derecho de cancelación de datos de carácter personal..

Artículo 15. Derecho de acceso.

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Por su parte, la ley también interviene regulando específicamente el tratamiento de datos de los menores de edad por parte de las entidades suministradoras de productos o servicios que vayan dirigidos a ellos o de los cuales puedan ser destinatarios como se refleja en la **Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, que modifica parcialmente el Código Civil y la Ley de Enjuiciamiento Civil**, establece que los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen incluyendo también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones. A su vez, la difusión de información, utilización de imágenes o nombre de los menores en los medios de comunicación, que puedan implicar una intromisión ilegítima en su intimidad, honor, propia imagen, o que sea contraria a sus intereses, determinará la intervención del Ministerio Fiscal, que instará de inmediato las medidas cautelares y de protección previstas en la Ley, tales como la retirada o bloqueo inmediato de los contenidos, solicitando inmediatamente las indemnizaciones que correspondan por los perjuicios causados.

Por otro lado, los menores tienen derecho a la libertad de expresión en los términos constitucionalmente previstos extendiéndose este derecho a los casos de publicación y difusión de sus opiniones, entre otros casos aunque dicha libertad debe ser limitada con el fin de proteger su intimidad y la propia imagen del menor.

Los menores tienen derecho a recibir asistencia adecuada que permita el efectivo ejercicio de sus derechos y que garanticen sus derechos, por ello el menor puede:

• Solicitar la protección y tutela ante el Defensor del Menor, la Fiscalía de Menores y la Consejería de Asuntos Sociales, así como de los Cuerpos y Fuerzas de Seguridad del Estado en los casos en los que sea necesario.

• Poner en conocimiento del Ministerio Fiscal las situaciones que considere que atentan contra sus derechos, con el fin de que éste promueva las acciones oportunas.

• Plantear sus quejas ante el Defensor del Pueblo, a fin de que dicha institución se haga cargo de modo permanente de los asuntos relacionados con los menores.

• Solicitar los recursos sociales de los que disponen las Administraciones Públicas.

A su vez, la **Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial**, establece en el **Artículo 22.3** que, en el orden civil, los juzgados y tribunales españoles serán competentes en materia de incapacitación y de medidas de protección de la persona o de los bienes de los menores o incapacitados, cuando éstos tuviesen su residencia habitual en España.

Respecto a las redes sociales, el punto que más controversia está causando en estas plataformas es que muchas de ellas están recabando datos de menores de 14 años sin consentimiento de padres o tutores y que la LOPD prohíbe. Igual que recabar datos del entorno familiar del menor, sea cual fuera su edad de ahí que en la actualidad sea mayor la presión por parte de las autoridades públicas y jurídicas a solicitar un compromiso por parte de los prestadores de servicios de Internet para implantar sistemas de verificación de la edad de los usuarios de las redes sociales, ya que muchas de estas redes mantienen perfiles de personas menores de 14 años.

Otras normativas que están relacionadas con las redes sociales y que pueden aplicarse cuando algunos de los derechos de los usuarios se vean vulnerados son:

- **Ley 1/1995 , de 27 de enero, de Protección del Menor**
- **Ley 10/ 1989, de 14 de diciembre, de Protección de Menores.**

3.2 Legislación Europea

El caso de Europa, el marco regulador para la privacidad en las redes sociales se base en principios generales de protección de datos. Incluso EEUU valora positivamente el modelo de la Directiva europea de Protección de Datos, frente a la gran cantidad de modelos legislativos que existen en Estados Unidos. Así pues, el marco regulador lo constituirán las leyes nacionales de protección de datos junto con la Directiva europea.

Para aproximarnos a la normativa de protección de datos europea es necesario acudir a los dictámenes y estudios jurídicos de la Agencia de protección de datos, en Europa es el **Grupo del artículo 29**, el cuál reúne a las principales agencias de protección de datos europeos y emite informes de gran interés. Este grupo ha ido creando una serie de

informes sobre la regulación en materia de redes sociales y en muchos de estos se encuentran los principios reguladores del futuro estándar internacional.

En primer lugar destaca, el **Memorándum de Roma del 2008** como el marco principal de referencia sobre redes sociales y privacidad; en este informe se intenta explicar porqué hay tan poca regulación sobre la publicación de datos personales. En dicho informe se recogen las principales recomendaciones del Grupo del artículo 29 del Memorándum de Roma a los juristas, entre ellas destacan:

- La introducción de un derecho para el uso de seudónimos.
- Asegurar que los proveedores de servicios sean honestos y transparentes en cuanto a la información requerida para estos servicios.
- El consentimiento de los menores deberá ser un aspecto importante a tratar , a fin de proteger sus derechos.
- Obligar a notificar cualquier tipo de riesgo para los datos personales que se puedan producir.
- Otorgar más responsabilidad a los proveedores sobre los datos personales en la Red.
- Introducir en la escuela la temática de la privacidad y de las herramientas protectoras.

En el año 2008 también se adoptó una resolución sobre la protección de la privacidad en los servicios de las redes sociales por parte de las agencias de protección de datos. De todas maneras, nos parece más relevante las recomendaciones de **ENISA (European Network and Information Security Agency) en el año 2007.**

Algunas de las recomendaciones que parecen más destacadas son:

- Las redes sociales deberían usar, una información adaptada al contexto, con el objetivo de acercarse a los usuarios de una manera más fiable.
- Las campañas de concienciación deberían ir dirigidas también a los programadores de software, con el fin de favorecer prácticas y políticas de empresa que respeten la privacidad.
- Es necesario realizar un estudio atento de la regulación que pueda aplicarse a las redes y revisar o dar respuesta adecuada a una serie de cuestiones que quedan en un vacío legal y tecnológico.

- Se debería informar a los usuarios de lo ocurre con los datos que publican antes y después de cerrar un perfil.
- Se debería tratar de manera controlada y transparente el boom de las redes, sin prohibir o desaconsejar, con campañas de sensibilización y concienciación dirigidas a los menores, a los profesores y a los padres.

El tercer documento relevante es el ***Working Paper*** **(n. º 163) del grupo de trabajo del artículo 29, sobre redes en línea, del 12 de junio del 2009**; en este informe habla sobre la Directiva de Bases de Datos Personales en el ámbito de las redes sociales, donde se exponen los siguientes puntos:

- Obligar a los proveedores a cumplir con la Directiva de protección de datos, e incluso la Directiva de e-privacidad, si son servicios donde se van a establecer comunicaciones Electrónicas.
- Obligar a los proveedores a informar de su identidad e indicar cuáles son las finalidades con las que se tratan los datos personales de los usuarios.
- Recomiendan que sólo se puedan colgar imágenes e información de terceros con el consentimiento de los individuos en cuestión.
- Los proveedores tendrían la obligación de advertir del derecho a la privacidad de los terceros.
- Cuando se obtengan datos sensibles, el proveedor deberá de obtener el consentimiento de forma explícita, salvo si fuera un dato público. Si la red social publica algún dato sensible en el perfil, debe dar constancia de que es con consentimiento de individuo. Las imágenes no serán un dato sensible, a menos que claramente sean usadas para revelar datos sensibles de los individuos.
- Respecto a los datos de terceros, los responsables de la Red deberían de informan acerca de la existencia de datos personales sobre él, aunque la comunicación mediante cualquier vía de comunicación sobre todo mediante correos electrónicos; podría vulnerar la prohibición del artículo 13.4 de la Directiva de E-privacidad, cuando se refiere al envío de mensajes electrónicos no solicitados para finalidades comerciales.
- Los servicios adicionales con los que cuentan algunas redes sociales y que utilizan los datos personales de usuarios, deberían estar advertidos de que deben de cumplir también las directivas de protección de datos personales.

- Recomiendan que la mejor herramienta para garantizar la privacidad es una buena seguridad y un funcionamiento garante de la privacidad (*privacy-friendly*) por defecto.
- También enuncian que las redes sociales deberían de proveerse de mejores mecanismos sin costes que favorecieran la privacidad de los usuarios(el problema que se le puede ver a este punto , es que si el usuario es el que decide que hacer con su información, es decir, los usuarios que quiere restringir y que son seleccionados por él mismo, la aceptación de otros usuarios independientemente de la relación que tengan o si cualquier dato que se publique se puede indexar en un motor de búsqueda) se estaría llevando a cabo un acceso público por lo que la legislación podría imponerle la Directiva de protección de datos, por la que se le asimilaría a las responsabilidades que adquiere un responsable de una base de datos puesto que no se trataría ya de un ámbito doméstico, sino público, incluso la libertad de expresión debería ser matizada con el debido respeto al derecho a la privacidad.
- Restringir el acceso a los perfiles desde los motores de búsqueda internos, con el fin de salvaguardar los datos personales de otros usuarios.
- La inclusión de medidas tecnológicas o *privacy enhancing technologies*:
- No solicitar datos sensibles en el formulario de suscripción; no dirigir el marketing directo a los menores; obtener el consentimiento previo de los padres o tutores; y separar la comunidad de menores de la de adultos.
- Desarrollar *privacy enhancing technologies* (PET), por ejemplo, avisos en forma de *pop-up* o ventanas en ciertos momentos determinantes, o software de verificación de la edad, etc.
- Establecer un código de conducta de los proveedores

En definitiva, en Europa no hay una normativa vigente pero si una serie de recomendaciones para las Agencias de Protección de Datos de los estados miembros a la hora de enfrentarse a la problemática de las redes sociales sobre todo a cuestiones que afectan a los derechos del individuo, que son los que hemos ido exponiendo a lo largo de la memoria.

4. Marco Tecnológico

En este capítulo hacemos un pequeño análisis de algunas tecnologías que podrían ser garantes de privacidad y que se podrían integrar en el acceso y uso de aplicaciones como redes sociales.

4.1. Tecnologías que integran privacidad

La información personal que contienen las redes sociales es de suma importancia a todos los niveles e incluso afecta al status económico en el sentido de que las redes sociales se han convertido en un negocio sustancial en el que también se ve afectada a la tecnología. Muchos juristas la consideran un riesgo para la privacidad sin embargo la realidad es otra muy distinta, muchos derechos que se llevan a cabo no podrían ejecutarse sin la intervención tecnológica como en el caso de la privacidad, se puede decir, que la seguridad y la privacidad no se conciben sin medidas técnicas.

El empleo de tecnología para proteger este derecho es de suma importancia a la hora progresar en el análisis de las redes sociales; en un principio se emplearon herramientas muy simples en su mayoría aquellas que tenían que ver con la teoría de grafos aunque cada vez se han ido creando más complejas incluyendo sistemas de reputación pero cada vez más lo medios sociales se enfrentan a nuevos riesgos cada vez más graves lo que ha propiciado que los tecnólogos y analistas en redes sociales creen nuevas tecnologías .

Existe una lucha continua entre tecnólogos y juristas para que estos acepten las recomendaciones de los primeros como una forma de proteger uno de los derechos principales del individuo "la privacidad" por ello, la investigación ha favorecido la extensión de las tecnologías garantes de la privacidad más tradicionales como la anonimización, la pseudoanonimización, y la autenticación hacia otras alternativas que hoy en día son muy valoradas por los expertos como las ***Privacy Enchancing Tecnologies (PETS)*** pero hay que tener en cuenta que estas no solucionan los problemas de privacidad sino que es necesario combinarlos con la gestión de la identidad y los sistemas de reputación.

Las ***Privacy Enchancing Tecnologies (PETS)*** también conocidas como tecnologías de la transparencia porque "deben de garantizar que el flujo de información sea visible y permita una trazabilidad "(**Roig Batalla, 2011),** son aquellas que garantizan a los usuarios el máximo control sobre los datos y se convierten en el eje principal para proteger la privacidad, además de ser una herramienta que contribuye a la mejora de la privacidad ayudado sin duda alguna por la implantación de normativas como es el caso de Europa donde dentro de la protección de datos se está haciendo primordial el control de la información. La siguiente ilustración, es un buen resumen gráfico de cómo las PETs son herramientas que permiten la protección de la privacidad.

Las ***Privacy Enchancing Tecnologies (PETS)*** a su vez integran mecanismos, herramientas y sistemas que permiten realizar una serie de funcionalidades que permiten también preservar la privacidad en la navegación.Algunos de estas tecnologías se pueden integrar en el uso de acceso y comunicación con aplicaciones de redes sociales y a través de web; como:

1. Hacer Pseudo-anónimas y Anónimas las Identidades

A continuación destacamos algunos de los softwares que llevan a cabo estas tareas entre los que destacan, Anonymizer (mejora el anonimato), el sitio más conocido es de pago pero tiene una versión libre con limitaciones. Además, le permite seguir los enlaces que se encuentran en las páginas a través de la misma navegación "privada" que se ha iniciado.

Por desgracia este sitio optó por cobrar por buena parte de sus servicios, aunque como hemos dichos, aún es posible utilizar una versión limitada gratuita. Las limitaciones de esta son una demora de 30 segundos en la descarga de la página, y acceso anónimo sólo a sitios con protocolo HTTP (no HTTPS ni FTP). Por otra parte, existen sitios que son inaccesibles a través de Anonymizer, como algunos servidores de e-mail por Web.

Otro servicio que nos puede prestar Anonymizer es acercarnos a páginas web lejanas, por ejemplo, si una página está ubicada en Japón y algún problema de enlace no nos permite conectarnos rápidamente (es decir: no la podemos ver), podemos pedirle a Anonymizer que entre a ella por nosotros y nos la muestre luego. Probablemente Anonymizer tenga un mejor enlace con Japón que el que tenemos nosotros, y esto nos

puede solucionar el problema. Anonymizer es una de las herramientas más populares para navegar anónimamente, pero no es la única.

2. TOR (Onion –Routing system)

Es el sistema de navegación anónima más popular basado en una red de "túneles" por las cuales los datos de navegación son cifrados y atraviesan múltiples nodos hasta llegar a su destino. Esto permite al usuario navegar anónimamente de forma que no se pueda rastrear la información que se envía. Este sistema de navegación cifra la información a su entrada y la descifra a la salida de dicha red, con lo cual es imposible saber quién envió la información aunque el propietario del servidor de salida si podría ver la información cuando es descifrada antes de llegar a Internet y acceder a la información aunque nunca conocerá al emisor del contenido.

3. NET Passport (Gestiona la Propiedad)

NET Passport es un servicio único que le permite usar una contraseña y un nombre de correo electrónico en los sitios afiliados a microsoft.com y en un número creciente de sitios Web participantes en Internet. Si tiene una cuenta .NET Passport, sólo tiene que recordar una contraseña y un nombre de inicio. Después de iniciar sesión en un sitio participante, puede hacerlo en todos los demás sitios participantes. Además, puede almacenar información sobre sí mismo en su perfil de inicio de sesión de .NET Passport, por lo que no tendrá que volver a escribirlo cuando visite los sitios participantes.

Una cuenta .NET Passport ayuda a proporcionar seguridad. La cuenta .NET Passport protege su información con una tecnología de cifrado poderosa y directivas de privacidad generales, permitiéndole controlar qué sitios tienen acceso a la información almacenada en su contraseña, incluyendo sus direcciones de correo electrónico y estándar, salvo en los casos que se describen en la Declaración de privacidad de .NET Passport.NET Passport hace también todo lo necesario para ayudar a proteger su intimidad en equipos públicos o compartidos. Por ejemplo, cuando cierra sesión toda su información personal relacionada con .NET Passport se elimina del equipo[7].

[7] En el siguiente enlace se puede obtener más información sobre las condiciones de NET Passport. http://www.passport.net

4. HTTP VERSUS HTTPS

En primer lugar pasaremos a definir HTTP, como el protocolo usado en cada transacción de la World Wide Web que define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, etc) para comunicarse, además está orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Mientras el HTTPS es un protocolo seguro de transferencia de hipertexto destinado a transferir datos de forma segura, y actualmente es el protocolo más utilizado por entidades bancarias, tiendas online, y cualquier servicio web que necesite el envío de datos personales o contraseñas para acceder , este protocolo cifra la información que se envía impidiendo que cualquier riesgo o ataque a través de cualquier programa pueda **descifrar** nuestras claves , por ejemplo en el caso de Facebook es más seguro que empleemos HTPPS que HTTP porque puede ocurrir el caso de que nos conectamos desde una red wifi no segura , si lo hacemos con HTTP corremos el riesgo de que cualquier persona acceda a nuestro perfil mientras con el protocolo HTTPS , la información quedará protegida mediante cifrado .Lo mismo ocurre en otras redes sociales donde quedan volcados y registrados datos personales por esta razón los administradores de estos medios sociales cada vez más incorporan este tipo de protocolos en sus opciones de seguridad ; como: Google+ donde el protocolo es utilizado para todo, en Twitter es opcional en la configuración de nuestra cuenta al igual que Facebook , y en Tuenti no se tiene posibilidad alguna de utilizarlo.

5. P3P

P3P (Platform for Privacy Preferences) los usuarios declaran su política de privacidad en sus navegadores, La **Plataforma de Preferencias de Privacidad** (Platform for Privacy Preferences) o P3P es un **protocolo que permite a los sitios web declarar el uso de la información que recopilan acerca de los usuarios que lo visitan**. Fue diseñado para dar a los usuarios más control sobre su información personal cuando navegan. P3P fue desarrollado por el World Wide Web Consortium (W3C) y se recomendó oficialmente el 16 de abril de 2002.

La privacidad de los datos personales que se manejan en Internet es una preocupación constante para empresas, gobiernos, medios de comunicación y el público en general. En ocasiones, existe una especie de desconfianza hacia Internet que influye negativamente en el desarrollo del comercio basado en la Web. Para solucionar este problema surge P3P, **Plataforma de Preferencias de Privacidad** (Platform for Privacy Preferences), que nace ante la necesidad de garantizar la privacidad en una web cada vez más extensa. P3P es un lenguaje estándar que ofrece a los usuarios una forma sencilla y automatizada de controlar en mayor medida el uso que se hace de su información personal en los sitios web que visitan. Y sirve para desarrollar herramientas y servicios que ofrezcan a los usuarios un mayor control sobre la información personal que se maneja en Internet y, al mismo tiempo, aumentar la confianza entre los servicios Web y los usuarios; mejora el control del usuario al colocar políticas de privacidad donde los usuarios pueden encontrarlas, en un formato en el que los usuarios pueden entender y, lo más importante, con la posibilidad de que el usuario actúe sobre lo que ve.

En conclusión, P3P proporciona a los usuarios web facilidad y regularidad a la hora de decidir si quieren o no, y bajo qué circunstancia, revelar información personal y permite a los sitios Web trasladar sus prácticas de privacidad a un formato estandarizado y procesable por dispositivos (basado en XML) que puede ser recuperado de forma automática y que además puede ser interpretado fácilmente por los navegadores de los usuarios.

Una vez completada una simple configuración del servidor, el sitio Web informará automáticamente a los visitantes de la página que ese sitio Web es compatible con **P3P**. En el lado del usuario, P3P automáticamente busca y lee las políticas de privacidad del sitio Web. Un navegador equipado para utilizar P3P puede comprobar una política de privacidad de un sitio Web e informar al usuario sobre las prácticas de información de ese sitio. El navegador puede entonces comparar automáticamente la declaración con las preferencias de privacidad del usuario, pautas reguladoras u otra variedad de estándares legales desde todo el mundo.

6. Conclusiones

Las conclusiones, las hemos extraído atendiendo a un criterio general donde observamos que las redes sociales han supuesto un gran fenómeno de expansión respecto a otros servicios de información online que han transformado la Web; una web que ha sufrido grandes cambios evolutivos desde unos sistemas más estáticos en la Web 1.0 hacía unos sistemas más dinámicos e interactivos en la Web 2.0, como es el caso de las redes sociales. Los usuarios han ido adquiriendo con el tiempo aptitudes o capacidades que anteriormente no poseían, han pasado de ser meros consumidores de información a ser ellos quien comuniquen, publiquen y compartan contenidos a través de Internet y sin duda las redes sociales son las herramientas que cumplen con todos estos requisitos, son los testigos de un cambio en la forma de comunicarse y de transmitir información no solo a través de un ordenados sino de dispositivos móviles. Dichas plataformas han ido creciendo conforme la vida actual va avanzando y cambiando, es decir, han irrumpido con fuerza sobre todo en los diferentes grupos sociales que forman esta sociedad tan inmersa en las nuevas tecnologías; las redes sociales nos permiten analizar los nuevos comportamientos de los individuos así como sus relaciones sociales.

Su popularidad va en aumento conforme el nivel de intercambio de contenidos de la Red, de ahí su expansión en todos los ámbitos sociales incluido el ámbito empresarial, al que ha aportado un sistema más ágil y eficaz de comunicación interna. En general, todos nos hemos rendido a sus encantos pero quizás no nos hayamos percatado tanto de los peligros o ataques malintencionados que pueden provocar en una serie de derechos que el individuo tiene garantizados por normativas jurídicas y que se vean vulnerados en estas plataformas de manera alarmante, a pesar de que dichas herramientas tienen mecanismos de control pero que en muchas ocasiones no son los adecuados.

Este tipo de situaciones está provocando enfrentamientos no solo a nivel de usuarios sino entre los proveedores de los servicios y los estados respecto a cuestiones relacionadas con la privacidad de los usuarios en este tipo de medios sociales, dicha razón está obligando a organismos tanto nacionales como internacionales a publicar guías e informes al respecto con el fin de adapatar distintas ideas y plasmarlas en las

legislaciones , sin embargo existe una gran diferencia entre los estados miembros de la Unión Europea por lo que existe una gran descoordinación en la materia , no habiendo un centralización que lleve a una directiva adecuada y que no quede obsoleta como es el caso de la directiva 95/46/CE.

En España, la única normativa que confiere derechos a los individuos y a los responsable de los ficheros respecto a sus datos personales es la Ley Orgánica de Protección de Datos y la Agencia Española de Protección de Datos es la encargada de velar por el cumplimiento de esta ley y de sancionar si se incumple, además es el único organismo que tiene un contacto directo con los representantes de distintas plataformas para que éstas sean más seguras respecto a la privacidad, pero el camino es muy largo y abrupto. La mayoría de las redes sociales incumplen la legalidad e incluso podrían mejorar muchos aspectos que protegiesen mejor los derechos de los usuarios. De todos los derechos que hemos ido exponiendo a lo largo del proyecto, alguno de ellos quedan cuestionados por la escasez legal o la controversia como la propiedad intelectual, ya que en muchas ocasiones es imposible dar una respuesta a aspectos técnicos con las exigencias legales; como por ejemplo la distribución constante de contenido protegido que los usuarios comparten sin que las plataformas puedan controlarlo, al igual que no se puede prohibir reproducir contenido con derechos de autor si luego eso no se puede controlar en dichas plataformas ni por la Ley ni por los prestadores de servicios por lo que se debería modificar o cambiar la legislación.

Hemos analizado algunas políticas de privacidad en concreto la red social más popular en nuestro país, donde hemos observado que los términos de acceso y de uso han ido cambiando desde el origen de las redes sociales hasta la actualidad, donde hay aspectos olvidados o más cuestionados como es el caso de la privacidad y por los que las redes sociales están intentando apostar a fin de seguir conservando a sus usuarios y garantizar su participación. Hay redes sociales que están haciendo esfuerzos para proteger por ejemplo a los menores (es el caso de Tuenti), los usuarios pueden eliminar los contenidos que aportan cuando este da de baja su perfil, además tiene una opción para poder configurar la privacidad aunque todavía queden ciertos aspectos en el aire. En Facebook se están llevando a cabo grandes los logros , es una red compleja en cuanto a la cantidad de aplicaciones y enlaces donde los usuarios tienen que compartir datos personales y muchas veces nosotros mismos perdemos el control de donde hemos

publicado y , el qué y si realmente la información difundida está guardada de modo seguro. Pero en parte muchas de las causas las provocamos nosotros mismos cuando no tomamos conciencia de lo que implica la participación en una red social y la desinformación, no leyendo las condiciones de uso o políticas de privacidad que las plataformas publican en estos sitios por lo que posteriormente tengamos consecuencias negativas.

En definitiva, la protección de la privacidad en las redes sociales no es la adecuada por varias razones:

- La legislación que protege al usuario es difícil de aplicar por estar fuera del ámbito jurisdiccional.
- Las redes sociales se amparan en políticas de uso y condiciones de registro por los que se exime de toda responsabilidad.
- No se exige por ley a los prestadores de servicios de redes sociales a que notifiquen cualquier tipo de riesgo que pueda poner en peligro los datos personales de los usuarios
- El marco regulador es inexistente o muy limitado, no es específico de las redes sociales sino al ámbito de internet o difusión pública como hemos visto anteriormente se limita a las regulaciones establecidas por algunas leyes, además de por las Agencias de protección de datos de los estados. A nivel europeo algún grupo de trabajo vinculado a la materia realiza informes y medidas en la materia que suplen el vacío legal.
  - No hay un estándar en normas para las prácticas de diseño y implementación de aplicaciones en redes sociales.
  - Los delitos que cometen los usuarios si están tipificados y penados.
  - Los delitos que cometen las redes sociales están establecidos fuera del territorio nacional.
  - Y por último, la tecnología garante de la privacidad en las redes sociales tiene una aparición muy débil, para algunos juristas es sinónimo de riesgo para los derechos del individuo y por eso no está fundamentada como garante de la privacidad a nivel jurídico en ninguna normativa.

7. Líneas Futuras de investigación

Una de las principales líneas de investigación que se deberían de llevar a cabo es la creación de un marco regulador común universal que recogiese una serie de principios únicos relacionados con las redes sociales y que se estudiasen aspectos que quedan exentos de la regulación jurídica y que afectan a la privacidad, como:

- ¿Qué deben de hacer los proveedores de servicios con los contenidos de los usuarios, una vez que estos dejan de participar en una red social? y cómo se podría regular.

- Investigar que sucede con la etiquetación, comentarios u opiniones que publican o comparten terceros en las redes sociales y como se regularía en las políticas de privacidad de las plataformas.

- ¿Cuál es el papel que deben de adoptar las Agencias de protección de datos para proteger los derechos de terceros que no forman parte de una red social, pero cuyos datos están publicados en dichos medios sin su consentimiento? ¿Y cómo se regularía?.
- Y por último, otras líneas de investigación que se podrían llevar a cabo es sobre cuestiones relativas a la suplantación de identidad de la que existe un vacío legal, o respecto a la localización de personas ¿cómo debería de protegerse?.

8. Bibliografía

Areito, J. (2010), *"Identificación y análisis en torno a la privacidad de la información: amenazas a las redes sociales"* [en línea], disponible en: http://www.redeweb.com/_txt/671/50.pdf [Consultado el 15 de Mayo].

Decreto (1996), *Real decreto legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual* [en línea], disponible en: http://noticias.juridicas.com/base_datos/Admin/rdleg1-1996.html [Consultado el 6 de Junio].

Decreto (2007), *Real decreto 1720/2007 de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la ley orgánica 15/1999, de protección de datos de carácter personal (RLOPD)* [en línea], disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf [Consultado el 11 de Julio].

Defensor del Menor de la Comunidad de Madrid (2011), "*Ciberbullying: Guía de recursos para centros educativos en casos de ciberacosos*" [en línea], disponible en: http://www.defensordelmenor.org/upload/documentacion/publicaciones/pdf/GUIA_Ciberbullying.pdf [Consultado el 20 de Julio].

Enisa (2007), *Security Issues and Recomendations for Online Social Networks* [en [en línea],disponible en: www.enisa.europa.eu/act/it/library/pp/soc-net/at_download/fullReport [Consultado el 7 de septiembre].

España, Agencia Nacional de Protección de Datos (2012)[en línea],disponible en : http://www.agpd.es/ [Consultado el 12 de mayo].

España, Instituto Nacional de Tecnologías de la Comunicación (2012) [en línea], disponible en: http://www.inteco.es/ [Consultado el 17 de mayo].

Facebook [en línea], disponible en: www.facebook.es [Consultado el 12 de septiembre].

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2009). *Dictamen 5/2009 sobre las redes sociales* [en línea], disponible en: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdf

Ley (1982), *Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y familiar y a la propia imagen* [en línea], disponible en: http://noticias.juridicas.com/base_datos/Admin/lo1-1982.html [Consultado el 12 de Junio].

Ley (1985), *Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial* [en línea], disponible en: http://noticias.juridicas.com/base_datos/Admin/lo6-1985.html [Consultado el 18 de Junio].

Ley (1989), *Ley 10/1989, de 14 de diciembre, de Protección de Menores* [en línea], disponible en: http://noticias.juridicas.com/base_datos/CCAA/ar-l10-1989.html [Consultado el 24 de Mayo].

Ley (1995), *Directiva europea 95/46 CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995 relativa a la Protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación* [en línea], disponible en: http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML [Consultado el 29 de Junio].

Ley (1995), *Ley 1/1995, de 27 de enero, de Protección del Menor* [en línea], disponible en: http://noticias.juridicas.com/base_datos/CCAA/as-l1-1995.html [Consultado el 25 de Mayo].

Ley (1995), *Ley orgánica 10/1995, de 23 de noviembre, del Código Penal* [en línea], disponible en: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html [Consultado el 29 de Mayo].

Ley (1996), *Ley orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor* [en línea], disponible en: http://noticias.juridicas.com/base_datos/Privado/lo1-1996.html [Consultado el 3 de Junio].

Ley (1999), *Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)* [en línea], disponible en: http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html [Consultado el 6 de Mayo].

Ley (2002), *Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la información y de Comercio Electrónico (LSSI-CE)* [en línea], disponible en: http://noticias.juridicas.com/base_datos/Admin/l34-2002.html [Consultado el 17 de Mayo].

Ley (2007), *Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones* [en línea], disponible en: http://noticias.juridicas.com/base_datos/Admin/l25-2007.html [Consultado el 24 de Mayo].

Informe (2009), *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales.* Madrid: INTECO [en línea], disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/estudio_inteco_aped_120209_redes_sociales.pdf [Consultado el 10 de Mayo].

Informe (2001), *Menores y Redes Sociales.* Madrid: Telefónica [en línea], disponible en: http://www.ite.educacion.es/es/inicio/ultimas-noticias/149-presentado-el-estudio-qmenores-y-redes-socialesq [Consultado el 25 de julio].

Martinez Martinez, R. (2010), *Derecho y redes sociales.* **Madrid:** CIVITAS-ARANZADI**,** pp.384.

Memoria (2012), *Monográfico de redes sociales de Isabel Ponce*. Madrid: INTECO [en línea], disponible en: http://recursostic.educacion.es/observatorio/web/es/internet/web-20/1043-redes-sociales?start=1 [Consulta 30 de Abril de 2012].

Presentación (2010), *Presentación sobre redes sociales y efectos Jurídicos* [en línea], disponible en: http://www.slideshare.net/lidiasanizo5/redes-sociales-y-efectos-juridicos-1995902 [Consulta 2 de Mayo de 2012].

Sánchez Ocaña, A. (2009), "¿*Existe la privacidad en las redes sociales?* [en línea], disponible en:
http://www.alejandrosuarez.es/2009/10/privacidad-en-redes-sociales/ [Consultado el 13 de Mayo].

Roig,A, (2009), "E-Privacidad y redes sociales". En: "V Congreso Internet, Derecho y Política (IPD).Cara y cruz de las redes sociales" [en línea], disponible en:
http://dialnet.unirioja.es/servlet/articulo?codigo=3101802 [Consultado el 29 de Mayo].

Vela Sánchez-Merlo, C. (2008), *"La privacidad de los datos en las redes sociales". Revista española de protección de datos,* 2008, Julio-Diciembre, n.5.